Command Reference for Cisco DSLAMs with NI-2

Cisco IOS Release 12.2DA
May 4, 2004

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-2073-02

Preface

This preface tells you who should read this document, how it is organized, and the document conventions it follows.

Audience

This document is written for anyone who installs or operates a Cisco digital subscriber line access multiplexer (DSLAM) with a second-generation network interface card (NI-2). Systems covered by this document include:

- Cisco 6015 DSLAM with NI-2
- Cisco 6100 DSLAM with NI-2
- Cisco 6130 DSLAM with NI-2
- Cisco 6160 DSLAM with NI-2
- Cisco 6260 DSLAM with NI-2

This guide does *not* cover:

- Cisco 6100 DSLAM with NI-1
- Cisco 6130 DSLAM with NI-1
- Cisco 6200 DSLAM
- Cisco 6400 aggregator

This book documents commands used to configure Cisco DSLAMs with NI-2. Commands in this book are listed alphabetically. For information on how to configure DSL features, refer to the *Configuration Guide for Cisco DSLAMs with NI-2*.

Note Commands that are identical to those documented in the *Cisco IOS Configuration Fundamentals Command Reference* and the *ATM and Layer 3 Switch Router Command Reference* have been removed from this document.

Note The port assignments and outputs of DSLAM commands are different than those in commands listed in the *ATM and Layer 3 Switch Router Command Reference*.

Document Organization

This guide is organized as follows:

- Chapter 1, “Cisco DSLAM User Interface”
- Chapter 2, “A Commands for Cisco DSLAMs with NI-2”
- Chapter 3, “C and D Commands for Cisco DSLAMs with NI-2”
- Chapter 4, “E Through M Commands for Cisco DSLAMs with NI-2”
- Chapter 5, “N Through shdsl Commands for Cisco DSLAMs with NI-2”
- Chapter 6, “Show Commands for Cisco DSLAMs with NI-2”
- Chapter 7, “Shutdown Through V Commands for Cisco DSLAMs with NI-2”

Document Conventions

Screen displays use the following convention:

^	The symbol ^ represents the key labeled Ctrl—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.

Command descriptions use the following conventions:

boldface font	Commands and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Alternative keywords are grouped in braces and separated by vertical bars.

Examples use the following conventions:

`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` `font`	Information you must enter is in **`boldface screen`** font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.

Notes and cautions use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

The software described in this guide runs on several Cisco DSLAM platforms, including the Cisco 6015, Cisco 6100, Cisco 6130, Cisco 6160, and Cisco 6260. This section lists hardware documents for each platform and software documents for all the platforms.

Hardware Documents

A complete list of all DSL hardware product related documentation is available on the World Wide Web at

http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/index.htm.

Software Documents

A complete list of all DSL IOS software product related documentation is available on the World Wide Web at

http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/ios_dsl/index.htm.

In the ATM software product related documentation, look for information pertaining to the Cisco LightStream 1010, which uses the same software base as the NI-2 DSL systems. This documentation is available on the World Wide Web at

http://www.cisco.com/univercd/cc/td/doc/product/atm/index.htm.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

Cisco DSLAM User Interface

This chapter describes the Cisco DSLAM user interface, provides instructions for using the command-line interface, and describes how to use the help system. The chapter also describes the command editing and command history features that you can use to recall previous command entries and edit previously entered commands.

This chapter includes the following sections:

Understanding the User Interface

The Cisco DSLAM user interface provides access to several different command modes, each with related commands. For security, the user interface provides three levels of access to commands:

- User mode—Called user EXEC mode.
- Privileged mode—The privileged mode is called privileged EXEC mode and requires a password.

  Note All commands that are available in user EXEC mode are also available in privileged EXEC mode; therefore, user EXEC mode is called EXEC mode in this guide.

  From the privileged EXEC mode, you can access global configuration mode and three specific configuration modes:

  – Terminal

  – Memory

  – Network configuration

- (ROM) monitor mode—This mode accesses a basic system kernel to which the Cisco DSLAM can default at startup if it does not find a valid system image, or if its configuration file is corrupted.

You can enter commands in uppercase, lowercase, or both. Only passwords are case sensitive. You can abbreviate commands and keywords to a unique number of characters. For example, you can abbreviate the **show** command to **sh**. After you enter the command line at the system prompt, press **Return** to execute the command.

Most configuration commands have a **no** form. In general, follow these guidelines:

- Use the **no** form of a command to disable a feature or function
- Use the command without the **no** keyword to re-enable a disabled feature or enable a feature that is disabled by default

You can use the context-sensitive help system to obtain a list of commands available for each command mode or a list of available options for a specific command by entering a question mark (**?**).

Accessing Command Modes

This section describes how to access the Cisco DSLAM command modes. Table 1-1 lists the following information:

- The command mode names.
- The method to access that mode.
- The prompt you see while in that mode. (For the purpose of this guide, the prompts use the default node name DSLAM.)
- The method to exit that mode.

Note Table 1-1 does not include all of the possible ways to access or exit each command mode.

Table 1-1 Command Modes

Command Mode	Access Method	Prompt	Exit Method
EXEC (user)	Log in to the switch or Cisco DSLAM.	`DSLAM>`	Use the **logout** command.
Privileged EXEC	From user EXEC mode, use the **enable** command and enter your password.	`DSLAM#`	To return to user EXEC mode, use the **disable** command.
ROM monitor	From privileged EXEC mode, use the **reload** command. Press **Break** during the first 60 seconds while the system boots.	`rommon` *x*`>`	The *x* represents the number of commands that have been entered at the DSLAM prompt. To exit ROM monitor mode, use the **cont** command.
Global configuration	From privileged EXEC mode, use the **configure** command. Use the keyword **terminal** to enter commands from your terminal.	`DSLAM(config)#`	To exit to privileged EXEC mode, use the **exit** or **end** command or press **Ctrl-Z**.

Table 1-1 Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method
Interface configuration	From global configuration mode, specify an interface with the **interface** command.	`DSLAM(config-if)#`	To exit to global configuration mode, use the **exit** command. To exit directly to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
Profile configuration	From global configuration mode, specify a profile with a **dsl-profile** command.	`DSLAM(cfg-dsl-profile)#`	To exit to global configuration mode, use the **exit** command. To exit directly to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
Line configuration	From global configuration mode, specify a management interface with a **line** command.	`DSLAM(config-line)#`	To exit to global configuration mode, use the **exit** command. To exit directly to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
ATM router configuration	From global configuration mode, configure the ATM router configuration with the **atm router pnni** command.	`DSLAM(config-atm-router)#`	To exit to global configuration mode, use the **exit** command. To exit directly to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
PNNI node configuration	From ATM router configuration mode, configure the PNNI routing node with the **node** command.	`DSLAM(config-pnni-node)#`	To exit to ATM router configuration mode, use the **exit** command. To exit directly to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
Auto-sync configuration	From global configuration mode, configure redundancy synchronization features with the **auto-sync** command.	`DSLAM(config-auto-sync)`	To exit to global configuration mode, use the **exit** command. To exit directly to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
Redundancy configuration	From global configuration mode, configure additional redundancy options with the **redundancy** command.	`DSLAM(config-red)`	To exit to global configuration mode, use the **exit** command. To exit directly to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.

Table 1-1 Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method
VRF configuration	From global configuration mode, configure a VPN routing/forwarding (VRF) routing table with the **ip vrf** command.	`DSLAM(config-vrf)`	To exit to global configuration mode, use the **exit** command. To exit directly to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
DHCP pool configuration	From global configuration mode, configure the DHCP address pool name and use the **ip dhcp pool** command to enter the DHCP pool configuration mode.	`DSLAM(dhcp-config)`	To exit to global configuration mode, use the **exit** command. To exit directly to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
ATM accounting file configuration	From global configuration mode, use the **atm accounting file** command to define an ATM accounting file.	`DSLAM(config-acct-file)#`	To exit to global configuration mode, use the **exit** command. To exit directly to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
ATM accounting selection configuration	From global configuration mode, use the **atm accounting selection** command to define an ATM accounting selection table entry.	`DSLAM(config-acct-sel)#`	To exit to global configuration mode, use the **exit** command. To exit directly to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.
ATM E.164 translation table configuration	From global configuration mode, enter the **atm e164 translation-table** command.	`DSLAM(config-atm-e164)`	To exit to privileged EXEC mode, use the **exit** command, **end** command, or press **Ctrl-Z**.
ATM signaling diagnostics configuration	From global configuration mode, enter the command **atm signalling diagnostics** and an index to configure.	`DSLAM(cfg-atmsig-diag)`	To exit to global configuration mode, use the **exit** command. To exit directly to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.

Understanding Command Modes

This section describes the various command modes and their levels of user access, including:

User EXEC Mode

When you log in to the Cisco DSLAM, you are in user EXEC, or simply EXEC, command mode. The EXEC mode commands available at the user level are a subset of those available at the privileged level. In general, the user EXEC mode commands allow you to connect to remote switches, change terminal settings on a temporary basis, perform basic tests, and list system information.

The user EXEC mode prompt consists of the DSLAM host name followed by the angle bracket (>):

```
Frodo>
```

or

```
DSLAM>
```

The default host name is DSLAM, unless you used the **host name** global configuration command to change the name of the host.

Privileged EXEC Mode

The privileged EXEC mode command set includes all user EXEC mode commands and the **configure** command, through which you can access global configuration mode and the remaining configuration submodes. Privileged EXEC mode also includes high-level testing commands, such as **debug**, and commands that display potentially secure information.

To enter or exit privileged EXEC mode, follow these steps:

	Command	Task
Step 1	`DSLAM> enable` `Password:password`	Enter privileged EXEC mode from EXEC mode.[1]
Step 2	`DSLAM#`	Enter privileged EXEC commands.
Step 3	`DSLAM# disable` `DSLAM>`	Exit privileged EXEC mode and return to EXEC mode.[2]

1. The prompt changes to the DSLAM host name followed by the pound sign (#).
2. The prompt changes back to the DSLAM host name followed by the angle bracket (>).

The system administrator uses the **enable password** global configuration command to set the password, which is case sensitive. If an enable password was not set, you can access privileged EXEC mode only from the console.

ROM Monitor Mode

ROM monitor mode provides access to a basic system kernel from which you can boot the Cisco DSLAM or perform diagnostic tests. The system can enter ROM mode automatically if the Cisco DSLAM does not find a valid system image, or if the configuration file is corrupted. The ROM monitor prompt is rommon *x*> without the DSLAM host name. The *x* represents the number of commands entered into the prompt.

You can also enter ROM monitor mode by intentionally interrupting the boot sequence by using the **Break** key during loading.

To return to EXEC mode from ROM monitor mode, use the **cont** command:

```
rommon 1> cont
DSLAM>
```

Global Configuration Mode

Global configuration mode provides access to commands that apply to the entire system. From global configuration mode, you can also enter the other configuration modes described in these sections.

	Command	Task

Step 1	`DSLAM# configure`
	or
	`DSLAM# configure terminal`
		Enter global configuration mode from privileged EXEC mode.
		Note You will not need to perform step 2 if you use the **configure terminal** command.

Step 2	`Configuring from terminal, memory, or network [terminal]? <CR>`	Specify the source of the configuration commands at the prompt. You can specify either the terminal, NVRAM, or a file stored on a network server as the source of configuration commands. The default is to enter commands from the terminal console.
Step 3	`DSLAM(config)#`	Enter configuration commands. The prompt changes to (config)#.
Step 4	`DSLAM(config)# exit`	Exit global configuration mode and return to privileged EXEC mode.

Interface Configuration Mode

Interface configuration mode provides access to commands that apply to an interface. Use these commands to modify the operation of an interface such as an ATM, Ethernet, or asynchronous port.

	Command	Task
Step 1	`DSLAM# configure terminal`	Go to global configuration mode.
Step 2	`DSLAM(config)# interface interface-type interface-number`	Enter interface configuration mode from global configuration mode. The prompt changes to (config-if)#.
Step 3	`DSLAM(config-if)# exit`	Exit interface configuration mode and return to global configuration mode. Enter **end** to return to privileged EXEC mode.

Profile Mode

Profile mode provides access to DSL profile commands. (See "Using DSL Profiles.")

	Command	Task
Step 1	`DSLAM# configure terminal`	Go to global configuration mode.
Step 2	`DSLAM(config)# dsl-profile profile-name`	Enter profile configuration mode and specify a profile. The prompt changes to (cfg-dsl-profile)#.
Step 3	`DSLAM(cfg-dsl-profile)# exit`	Exit profile mode and return to global configuration mode. Enter **end** to return to privileged EXEC mode.

Line Configuration Mode

Line configuration mode provides access to commands used to configure lines on the DSLAM.

	Command	Task
Step 1	`DSLAM# configure terminal`	Go to global configuration mode.
Step 2	`DSLAM(config)# line line-index`	Enter line configuration mode from global configuration mode. The prompt changes to (config-line)#.
Step 3	`DSLAM(config-line)# exit`	Exit profile mode and return to global configuration mode. Enter **end** to return to privileged EXEC mode.

ATM Router Configuration Mode

ATM router configuration mode provides access to commands that you use to configure Private Network-to-Network Interface (PNNI) routing.

	Command	Task
Step 1	`DSLAM# configure terminal`	Go to global configuration mode.
Step 2	`DSLAM(config)# atm router pnni`	Enter ATM router configuration mode from global configuration mode. The prompt changes to (config-atm-router)#.
Step 3	`DSLAM(config-atm-router)# exit`	Exit ATM router configuration mode and return to global configuration mode. Enter **end** to return to privileged EXEC mode.

PNNI Node Configuration Mode

The PNNI node configuration mode is a submode of ATM router configuration mode and provides access to commands that you use to configure PNNI nodes on the Cisco DSLAM.

	Command	Task
Step 1	`DSLAM# configure terminal`	Go to global configuration mode.
Step 2	`DSLAM(config)# atm router pnni`	Enter ATM router configuration mode from global configuration mode. The prompt changes to (config-atm-router)#.
Step 3	`DSLAM(config-atm-router)# node` *node-index*	Enter PNNI node configuration mode from global configuration mode. The prompt changes to (config-pnni-node)#.
Step 4	`DSLAM(config-pnni-node)# exit`	Exit PNNI node configuration mode and return to global configuration mode. Enter **end** to return to privileged EXEC mode.

Redundancy Configuration Mode

The redundancy configuration mode provides access to commands that you use to configure redundancy on the DSLAM.

	Command	Task
Step 1	`DSLAM# configure terminal`	Go to global configuration mode.
Step 2	`DSLAM(config)# redundancy`	Enter redundancy configuration mode from global configuration mode. The prompt changes to (config-red)#.
Step 3	`DSLAM(config-red)# exit`	Exit redundancy configuration mode and return to global configuration mode. Enter **end** to return to privileged EXEC mode.

VRF Configuration Mode

The VPN routing/forwarding instance (VRF) configuration mode provides access to commands that you use to configure a VRF on the DSLAM.

	Command	Task
Step 1	`DSLAM# configure terminal`	Go to global configuration mode.
Step 2	`DSLAM(config)# ip vrf` *vrf-name*	Enter VRF configuration mode from global configuration mode. The prompt changes to (config-vrf)#.
Step 3	`DSLAM(config-vrf)# exit`	Exit VRF configuration mode and return to global configuration mode. Enter **end** to return to privileged EXEC mode.

DHCP Pool Configuration Mode

The DHCP configuration mode provides access to commands that you use to configure a DHCP server on the DSLAM.

	Command	Task
Step 1	`DSLAM# configure terminal`	Go to global configuration mode.
Step 2	`DSLAM(config)# ip dhcp pool` *name*	DHCP pool configuration mode from global configuration mode. The prompt changes to (config-dhcp)#.
Step 3	`DSLAM(config-dhcp)# exit`	Exit DHCP configuration mode and return to global configuration mode. Enter **end** to return to privileged EXEC mode.

ATM Accounting File Configuration Mode

ATM accounting file configuration mode provides access to commands that you use to configure a file for accounting and billing of virtual circuits (VCs).

	Command	Task
Step 1	`DSLAM# configure terminal`	Go to global configuration mode.
Step 2	`DSLAM(config)# atm accounting file` *accounting-filename*	Enter ATM accounting file configuration mode from global configuration mode. The prompt changes to (config-acct-file)#.
Step 3	`DSLAM(config-acct-file)# exit`	Exit ATM accounting file configuration mode and return to global configuration mode. Enter **end** to return to privileged EXEC mode.

ATM Accounting Selection Configuration Mode

ATM accounting selection configuration mode provides access to commands that you use to specify the connection data that the DSLAM will gather.

	Command	Task
Step 1	`DSLAM# configure terminal`	Go to global configuration mode.

	Command	Task
Step 2	`DSLAM(config)# atm accounting selection` *accounting-selection-index*	Enter ATM accounting selection configuration mode from global configuration mode. The prompt changes to (config-acct-sel)#.
Step 3	`DSLAM(config-acct-sel)# exit`	Exit ATM accounting selection configuration mode and return to global configuration mode. Enter **end** to return to privileged EXEC mode.

ATM E.164 Translation Table Configuration Mode

ATM E.164 translation table configuration mode provides access to commands that you use to configure the translation table that maps native E.164 format addresses to ATM end system (AESA) format addresses.

	Command	Task
Step 1	`DSLAM# configure terminal`	Go to global configuration mode.
Step 2	`DSLAM(config)# atm e164 translation-table`	Enter ATM E.164 translation table configuration mode from global configuration mode. The prompt changes to (config-atm-e164)#.

Step 3	`DSLAM(config-atm-e164)# exit`
	or
	`DSLAM(config-atm-e164)# end`
		Exit ATM E.164 translation table configuration mode and return to privileged EXEC mode.

ATM Signaling Diagnostics Configuration Mode

ATM signaling diagnostics configuration mode provides access to commands that you use to configure the signaling diagnostics table.

	Command	Task
Step 1	`DSLAM# configure terminal`	Go to global configuration mode.
Step 2	`DSLAM(config)# atm signalling diagnostics`	Enter ATM signaling diagnostics configuration mode. The prompt changes to (cfg-atmsig-diag).
Step 3	`DSLAM(cfg-atmsig-diag)# exit`	Exit ATM signaling diagnostics configuration mode and return to global configuration mode. Enter **end** to return to privileged EXEC mode.

Using Context-Sensitive Help

The user interface provides context-sensitive help in all modes. This section describes how to configure and display context-sensitive help.

Configuring Help for Terminal Sessions

The following commands configure full help.

Command	Task
DSLAM# **terminal full-help**	In privileged EXEC mode, configure the current terminal session to receive help for the full set of user-level commands.
DSLAM(config-line)# **full-help**	In line configuration mode, configure a specific line to allow users without privileged access to obtain full help.

Displaying Context-Sensitive Help

To get help that is specific to a command mode, a command, a keyword, or an argument, perform one of these tasks:

Command	Task
help	Obtain a brief description of the help system in any command mode.
abbreviated-command-entry?	Obtain a list of commands that begin with a particular character string.
abbreviated-command-entry<**Tab**>	Complete a partial command name.
?	List all commands available for a particular command mode.
command **?**	List the associated keywords of a command.
command keyword **?**	List the associated arguments a keyword.

Using Word Help

To view a list of commands that begin with a particular character sequence, type those characters followed immediately by the question mark (?). Do not include a space. This form of help is called *word help*, because it completes a word for you.

In this example, the system displays the possible commands in privileged EXEC mode that begin with “co.”

```
DSLAM# co?
configure  connect  copy
```

This feature helps you determine the minimum subset that you can use when you abbreviate a command.

Command Syntax Help

To list keywords or arguments, enter a question mark (**?**) in place of a keyword or argument. Include a space before the **?**. This form of help is called *command syntax help,* because it reminds you which keywords or arguments are applicable, based on the command, keywords, and arguments you have already entered.

This example demonstrates the use of command syntax help to complete the **access-list** command. Entering the question mark (**?**) displays the allowed arguments:

```
DSLAM(config)# access-list ?
  <1-99>     IP standard access list
  <100-199>  IP extended access list
```

Enter the access list number, **99**, followed by a question mark (**?**) to display the allowed keywords:

```
DSLAM(config)# access-list 99 ?
  deny    Specify packets to reject
  permit  Specify packets to forward
```

Enter the **deny** argument followed by a question mark (**?**) to display the next argument (host name or IP address) and two keywords:

```
DSLAM(config)# access-list 99 deny ?
  Hostname or A.B.C.D  Address to match
  any                  Any source host
  host                 A single host address
```

Enter the IP address followed by a question mark (**?**) to display a final (optional) argument. The <CR> indicates that you can press **Return** to execute the command:

```
DSLAM(config)# access-list 99 deny 131.108.134.0 ?
  A.B.C.D  Wildcard bits
  <cr>
DSLAM(config)# <cr>
```

The system adds an entry to access list 99 that denies access to all hosts on subnet 131.108.134.0.

Checking Command Syntax

The user interface provides an error indicator (^) that appears in the command string in which you have entered an incorrect or incomplete command, keyword, or argument.

This example shows a command entry that is correct up to the last element:

```
DSLAM# clock set 13:04:30 28 apr 98
                                 ^
% Invalid input detected at '^' marker.
```

The caret symbol (^) and help response indicate the location in which the error occurs. To list the correct syntax, reenter the command, substituting a question mark (**?**) where the error occurred:

```
DSLAM# clock set 13:32:00 23 February ?
  <1993-2035> Year
DSLAM# clock set 13:32:00 23 February
```

Enter the year using the correct syntax and press **Enter** to execute the command:

```
DSLAM# clock set 13:32:00 23 February 1993
```

Using the Command History Features

The user interface provides a history or record of commands you enter. You can use the command history feature for recalling long or complex commands or entries, including access lists. With the command history feature, you can complete the following tasks:

- Setting the Command History Buffer Size, page 1-13
- Recalling Commands, page 1-13
- Disabling the Command History Feature, page 1-14

Setting the Command History Buffer Size

By default, the system records ten command lines in its history buffer. Use the following commands to set the number of command lines the system records.

Command	Task
`DSLAM# terminal history [size number-of-lines]`	In privileged EXEC mode, enable the command history feature for the current terminal session.
`DSLAM(config-line)# history [size number-of-lines]`	In line configuration mode, enable the command history feature for a specific line.

Recalling Commands

To recall commands from the history buffer, perform one of these tasks:

Key Sequence/Command	Task
Press **Ctrl-P** or the up arrow key.[1]	Recall commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall each previous command that you entered.
Press **Ctrl-N** or the down arrow key.[1]	Return to more recent commands in the history buffer after you recall commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.
`DSLAM> show history`	While in EXEC mode, list the last several commands you have just entered.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Disabling the Command History Feature

The command history feature is automatically enabled. Use the following commands to disable it.

Command	Task
`DSLAM> terminal no history`	In EXEC mode, disable the command history feature for the current terminal session.
`DSLAM(config-line)# no history`	In line configuration mode, configure the line to disable the command history feature.

Using the Editing Features

The user interface includes an enhanced editing mode that provides a set of editing key functions similar to those of the Emacs editor.

Using the editing features, you can perform the following tasks:

Enabling Enhanced Editing Mode

Although the current software release enables the enhanced editing mode by default, you can disable it and revert to the editing mode of previous software releases. Use the following commands to reenable the enhanced editing mode.

Command	Task
`DSLAM> terminal editing`	In EXEC mode, enable the enhanced editing features for the current terminal session.
`DSLAM(config-line)# editing`	In line configuration mode, enable the enhanced editing features for a specific line.

Moving Around on the Command Line

Use these keystrokes to move the cursor around on the command line for corrections or changes:

Keystrokes	Task
Press **Ctrl-B** or press the **Left Arrow** key.[1]	Move the cursor back one character.
Press **Ctrl-F** or press the **Right Arrow** key.[1]	Move the cursor forward one character.
Press **Ctrl-A**.	Move the cursor to the beginning of the command line.
Press **Ctrl-E**.	Move the cursor to the end of the command line.
Press **Esc B**.	Move the cursor back one word.
Press **Esc F**.	Move the cursor forward one word.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Completing a Partial Command Name

If you cannot remember a complete command name, you can use **Tab** to allow the system to complete a partial entry:

Keystrokes	Task
Enter the first few letters and press **Tab**.	Complete a command name.

If your keyboard does not have **Tab**, press **Ctrl-I** instead.

In this example, when you enter the letters **conf** and press **Tab**, the system provides the complete command:

```
DSLAM# conf<Tab>
DSLAM# configure
```

If you enter an ambiguous set of characters, the system generates an error message. To display the list of legal commands beginning with the specified string, enter a question mark (**?**) after you see the error message. See the “Using Word Help” section on page 1-11.

Pasting in Buffer Entries

The system provides a buffer that contains the last ten items that you deleted. You can recall these items and paste them in the command line by using these keystrokes:

Keystrokes	Task
Press **Ctrl-Y**.	Recall the most recent entry in the buffer.
Press **Esc Y**.	Recall the next buffer entry.

The buffer contains only the last ten items that you have deleted or cut. If you press **Esc Y** more than 10 times, you cycle back to the first buffer entry.

Editing Command Lines That Wrap

The new editing command set provides a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. To scroll back, use these keystrokes:

Keystrokes	Task
Press **Ctrl-B** or the **Left Arrow** key[1] repeatedly.	Scroll back one character at a time to the beginning of a command line to verify that you entered a lengthy command correctly.
Press **Ctrl-A**.	Return directly to the beginning of the line.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

In this example, the **access-list** command entry extends beyond one line. When the cursor reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) indicates that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

```
DSLAM(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
DSLAM(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
DSLAM(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
DSLAM(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

When you complete the entry, press **Ctrl-A** to check the complete syntax before pressing **Return** to execute the command. The dollar sign ($) appears at the end of the line to indicate that the line has scrolled to the right:

```
DSLAM(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

The Cisco DSLAM default is a terminal screen that is 80 columns wide. If you have a width other than that, use the **terminal width** command to provide the correct width of your terminal.

Use line wrapping together with the command history feature to recall and modify previous complex command entries.

Deleting Entries

Use any of these keystrokes to delete command entries if you make a mistake or change your mind:

Keystrokes	Task
Press **Delete** or **Backspace**.	Erase the character to the left of the cursor.
Press **Ctrl-D**.	Delete the character at the cursor.
Press **Ctrl-K**.	Delete all characters from the cursor to the end of the command line.
Press **Ctrl-U** or **Ctrl-X**.	Delete all characters from the cursor to the beginning of the command line.

Keystrokes	Task
Press **Ctrl-W**.	Delete the word to the left of the cursor.
Press **Esc D**.	Delete from the cursor to the end of the word.

Scrolling Down a Line or a Screen

When you use the help facility to list the commands available in a particular mode, the list is often longer than the terminal screen can display. In such cases, a More prompt appears at the bottom of the screen. To respond to the More prompt, use these keystrokes:

Keystrokes	Task
Press **Return**.	Scroll down one line.
Press **Space**.	Scroll down one screen.
Press **Esc**.	Stop scrolling and return to the main prompt.

Redisplaying the Current Command Line

If you enter a command and a message appears on your screen, you can easily recall your current command line entry. To do so, use these keystrokes:

Keystrokes	Task
Press **Ctrl-L** or **Ctrl-R**.	Redisplay the current command line.

Transposing Mistyped Characters

If you have mistyped a command entry, you can transpose the mistyped characters by using these keystrokes:

Keystrokes	Task
Press **Ctrl-T**.	Transpose the character to the left of the cursor and the character located at the cursor.

Controlling Capitalization

You can capitalize a word, set a word to lowercase, or capitalize a set of letters with these keystrokes:

Keystrokes	Task
Press **Esc C**.	Capitalize at the cursor.
Press **Esc L**.	Change the word at the cursor to lowercase.
Press **Esc U**.	Capitalize letters from the cursor to the end of the word.

Designating a Keystroke as a Command Entry

To use a particular keystroke as an executable command, insert a system code:

Keystrokes	Task
Press **Ctrl-V** or **Esc Q**.	Insert a code to indicate to the system that it should treat the following keystroke as a command entry, *not* an editing key.

Disabling Enhanced Editing Mode

To disable enhanced editing mode and revert to the normal editing mode, use this command in privileged EXEC mode:

Command	Task
`DSLAM# terminal no editing`	Disable the enhanced editing features for the local line.

If you have prebuilt scripts that do not interact well when enhanced editing is enabled, you can disable enhanced editing mode. To reenable enhanced editing mode, use the **terminal editing** command.

Ending a Session

After you use the **setup** command or other configuration command, exit the Cisco DSLAM and quit the session.

To end a session, use this EXEC command:

Command	Task
`DSLAM> quit`	End the session.

A Commands for Cisco DSLAMs with NI-2

This chapter documents commands that you use to configure Cisco DSLAMs with NI-2. Commands in this chapter are listed alphabetically. For information on how to configure DSL features, refer to the *Configuration Guide for Cisco DSLAMs with NI-2*.

Note Commands that are identical to those documented in the *Cisco IOS Configuration Fundamentals Command Reference* and the *ATM and Layer 3 Switch Router Command Reference* have been removed from this chapter.

This chapter discusses the following commands:

aaa authentication ppp

aaa authorization

aaa new-model

accept-dialin

address-family

alarms

aps clear

aps force

aps lockout

aps manual

atm clp-drop

atm connection-traffic-table-row

atm input-queue

atm input-threshold

atm ni2-switch trunk

atm oam intercept segment

atm pvc

atm pvp

atm route-bridged

atm soft-vc

atm soft-vp

auto-sync

aaa authentication ppp

To specify one or more AAA authentication methods for use on ATM and DSL interfaces running PPP, use the **aaa authentication ppp** global configuration command. Use the **no** form of this command to disable authentication.

aaa authentication ppp {default | list-name} method1 [...[method4]]

no aaa authentication ppp {default | list-name} method1 [...[method4]]

Syntax Description

default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
list-name	Character string that you use to name the list of authentication methods tried when a user logs in.
method	At least one and up to four of the keywords described in Table 2-1.

Defaults

If the default list is not set, only the local user database is checked. This version has the same effect as the following command:

aaa authentication ppp default local

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The system uses lists that you create by using the aaa authentication ppp command with the ppp authentication command. These lists contain up to three authentication methods that the system uses when a user tries to log in to the serial interface.

Create a list by entering the **aaa authentication ppp** list-name method command, where list-name is any character string used to name this list, such as MIS-access. The method argument identifies the list of methods the authentication algorithm tries in the given sequence. You can enter up to four methods. Method keywords are described in Table 2-1.

The additional methods of authentication are used only if the previous method returns an error, not if it fails. Specify *none* as the final method in the command line to have authentication succeed even if all methods return an error.

If authentication is not specifically set for a function, the default is none and no authentication is performed. Use the **show running-config** command to view lists of authentication methods.

Table 2-1 AAA Authentication PPP Method Descriptions

Keyword	Description
if-needed	Does not authenticate if user has already been authenticated on a TTY line
group	Uses the group-server for authentication
local	Uses the local username database for authentication
local-case	Uses case-sensitive local username authentication
none	Uses no authentication

Examples

The following example creates an AAA authentication list called MIS-access for serial lines that use PPP. The user is allowed access with no authentication.

```
DSLAM(config)# aaa new-model
DSLAM(config)# aaa authentication ppp mis-access group radius
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
ppp authentication	Enables Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) and enables an AAA authentication method on an interface.

aaa authorization

To set parameters that restrict a user's network access, use the **aaa authorization** global configuration command. To disable authorization for a function, use the **no** form of this command.

aaa authorization {**network** | **exec** | **commands** *level* | **reverse-access | auth-proxy**} {**default** | *list-name*} [*method1* [*method2...*]]

no aaa authorization {**network** | **exec** | **commands** *level* | **reverse-access | auth-proxy**}

Syntax Description

network	Runs authorization for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARA.
exec	Runs authorization to determine if the user is allowed to run an EXEC shell. This facility might return user profile information such as **autocommand** information.
commands	Runs authorization for all commands at the specified privilege level.
level	Specifies command level that should be authorized. Valid entries are 0 through 15.
reverse-access	Runs authorization for reverse access connections, such as reverse Telnet.
auth-proxy	Runs authorization for the authentication proxy.
default	Uses the listed authorization methods that follow this argument as the default list of methods for authorization.
list-name	Use this character string to name the list of authorization methods.
method1 [method2...]	One of the keywords listed in Table 2-2.

Defaults

Authorization is disabled for all actions (equivalent to the method keyword **none**). If you issue the **aaa authorization** command for a particular authorization type without specifying a named method list , the system automatically applies the default method list to all interfaces or lines (where this authorization type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If you do not define a default method list, then no authorization takes place.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

Use the **aaa authorization** command to enable authorization and to create named method lists that define authorization methods for user access to the specified function. Method lists for authorization define the ways that the system performs authorization and the sequence in which the system performs these methods. A method list is a named list that describes the authorization methods to be queried (such as RADIUS), in sequence. You can use method lists to designate one or more security protocols that are

to be used for authorization, thus ensuring a backup system if the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until communication with a listed authorization method succeeds, or all methods defined are exhausted.

Note The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle—meaning that the security server or local username database responds by denying the user services—the authorization process stops and no other authorization methods are attempted.

Use the **aaa authorization** command to create a list by entering the *list-name* and the *method*, where *list-name* is any character string that is used to name this list (excluding all method names) and *method* identifies the list of authorization method(s) tried in the given sequence.

Method keywords are described in Table 2-2.

Table 2-2 Authorization Methods

Method Keyword	Description
if-authenticated	Allows the user to access the requested function if the user is authenticated.
none	No authorization is performed.
local	Uses the local database for authorization.
group	Uses server-group for authorization information.

Cisco IOS software supports the following five methods for authorization:

- **If-Authenticated**—The user can access the requested function if the user was authenticated successfully. Not supported with the **auth-proxy** authorization type.
- **None**—The network access server does not request authorization information; authorization is not performed over this line/interface. Not supported with the **auth-proxy** authorization type.
- **Local**—The router or access server consults its local database, as defined by the **username** command, to authorize specific rights for users. The local database can control only a limited set of functions. Not supported with the **auth-proxy** authorization type.
- **RADIUS**—The network access server requests authorization information from the RADIUS security server. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
- **Kerberos Instance Map**—The network access server uses the instance that the **kerberos instance map** command defines for authorization. Not supported with the **auth-proxy** authorization type.

Method lists are specific to the type of authorization being requested. AAA supports five different types of authorization:

- **Network**—Applies to network connections which can include a PPP, SLIP, or ARA connection.
- **EXEC**—Applies to the attributes that are associated with a user EXEC terminal session.
- **Commands**—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.

- **Reverse Access**—Applies to reverse Telnet sessions.
- **Auth-proxy**—Applies to HTTP sessions that trigger the authentication proxy feature.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

After you define them, you must apply method lists to specific lines or interfaces before any defined method is performed.

The authorization command causes a request packet that contains a series of AV pairs to be sent to the RADIUS server as part of the authorization process. The server can do one of the following:

- Accept the request as is
- Make changes to the request
- Refuse the request and refuse authorization

For a list of supported RADIUS attributes, refer to the RADIUS attributes appendix in the *Security Configuration Guide*.

Note Five commands are associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will be excluded from the privilege level command set.

When you enable the authentication proxy, the AAA server, you must configure the database used for authentication and the authentication proxy service for authorization.

Note Use the **ip auth-proxy name** command in conjunction with the **aaa authorization auth-proxy** command. Together these commands set up the authorization policy that the firewall can download.

Examples

In this example, the first method of authorization using the authentication proxy is RADIUS.

```
DSLAM(config)# aaa new-model
DSLAM(config)# aaa authorization auth-proxy default group radius
```

The following example shows the **aaa authorization auth-proxy** command as part of an AAA new model configuration. Use these AAA configuration commands to secure the router when the authentication proxy is enabled. Failure to configure the router properly could result in security holes.

```
DSLAM(config)# aaa new-model
DSLAM(config)# aaa authentication login default group radius
DSLAM(config)# aaa authorization auth-proxy default group radius
```

Related Commands

Command	Description
aaa authentication	Specifies one or more AAA authentication methods for use on serial interfaces that run PPP.
aaa new-model	Enables the AAA access control mode.

aaa new-model

To enable the AAA access control model, issue the **aaa new-model** global configuration command. Use the **no** form of this command to disable this functionality.

aaa new-model

no aaa new-model

Syntax Description

This command has no arguments or keywords.

Defaults

AAA is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

This command enables the AAA access control system.

Examples

The following example initializes AAA:

```
DSLAM(config)# aaa new-model
```

Related Commands

Commands	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict a user's network access.
ppp authentication	Enables Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) and enables an AAA authentication method on an interface.

accept-dialin

To create an accept-dialin VPDN subgroup, use the **accept-dialin** VPDN group command. To remove the accept-dialin subgroup from a VPDN group, use the **no** form of this command.

accept-dialin

no accept-dialin

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

VPDN group mode

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

For a VPDN group to accept dial-in calls, you must also configure the:

- **terminate-from** VPDN group command
- **protocol** VPDN subgroup command
- **virtual-template accept-dialin** command

You must configure the **vpdn group** command with the **accept-dialin** or **request-dialin** command for the dial-in to be functional. The requester initiates a dial-in tunnel. The acceptor accepts a request for a dial-in tunnel.

Examples

If you do not use the **terminate-from** command, you automatically enable a default VPDN group, which allows all tunnels to share the same tunnel attributes:

```
DSLAM(config)# vpdn enable
DSLAM(config)# vpdn-group 1
! Default L2TP VPDN group
DSLAM(config-vpdn)# accept-dialin
DSLAM(config-vpdn-acc-in)# protocol l2tp
DSLAM(config-vpdn-acc-in)# virtual-template 1
```

Related Commands

Command	Description
protocol	Specifies the tunneling protocol that is used for the dial-in connections.
virtual-template	Specifies the interface that an accept-dialout group will use to dial out calls.

address-family

To enter the address family submode that configures routing protocols, such as BGP, RIP, and static routing, use the **address-family** global configuration command. To disable the address-family submode that configures routing protocols, use the **no** form of this command.

VPN-IPv4 unicast

address-family vpnv4 [**unicast**]

no address-family vpnv4 [**unicast**]

IPv4 unicast

address-family ipv4 [**unicast**]

no address-family ipv4 [**unicast**]

IPv4 unicast with CE router

address-family ipv4 [**unicast**] **vrf** *vrf-name*

no address-family ipv4 [**unicast**] **vrf** *vrf-name*

Syntax Description

Keyword	Description
ipv4	Sessions that carry standard IPv4 address prefixes.
vpnv4	Sessions that carry customer VPN-IPv4 prefixes, each of which is globally unique because of an 8-byte route distinguisher.
unicast	(Optional) Unicast prefixes.
vrf *vrf-name*	Name of a VPN routing or forwarding instance (VRF) to associate with submode commands.

Defaults

Routing information for address family IPv4 is advertised by default when you configure a BGP session using the **neighbor...remote-as** command, unless you execute the **no bgp default ipv4-activate** command.

Command Modes

Address-family configuration submode

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

When you use the **address-family** command, you enter address-family configuration submode (prompt: `(config-router-af)#`). Within this submode, you can configure address-family specific parameters for routing protocols, such as BGP, that can accommodate multiple Layer 3 address families.

To exit address-family configuration submode and return to router configuration mode, type **exit-address-family**, or **exit**.

Examples

The **address-family** command in the following example places the router into address-family configuration submode for the VPNv4 address family. Within the submode, you can configure advertisement of NLRI for the VPNv4 address family using the **neighbor activate** command and other related commands:

```
DSLAM(config)# router bgp 100
DSLAM(config-router)# address-family vpnv4
DSLAM(config-router-af)#
```

The command in the following example places the router into address-family configuration submode for the IPv4 address family. Use this form of the command, which specifies a VRF, only to configure routing exchanges between PE and CE devices. This address-family command causes subsequent commands that you enter in the submode to execute in the context of VRF vrf2. Within the submode, you can use the **neighbor activate** command and other related commands to accomplish the following:

- Configure advertisement of IPv4 NLRI between the PE and CE routers.
- Configure translation of the IPv4 NLRI (that is, translate IPv4 into VPNv4 for NLRI received from the CE, and translate VPNv4 into IPv4 for NLRI to be sent from the PE to the CE).
- Enter the routing parameters that apply to this VRF.

Enter the address-family configuration submode as follows:

```
DSLAM(config)# router bgp 100
DSLAM(config-router)# address-family ipv4 unicast vrf vrf2
DSLAM(config-router-af)#
```

Related Commands

Command	Description
exit-address-family	Exits address-family submode.
neighbor activate	Exchanges an address with a neighboring router.

alarms

To enable alarms in profile command mode, use the **alarms** command. To disable alarms, use the **no** form of the command.

alarms

no alarms

Syntax Description

This command has no keywords or arguments.

Defaults

Disabled

Command Modes

Profile configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

The command affects minor alarms for DSL subscriber ports only. The alarms that this command controls apply to these event classes:

- Near End LOS
- Near End LOCD
- Near End LOF
- Subscriber port failure
- Upstream or downstream bit rate not above minimum bit rate

When you enable or disable alarms, only the specified profile is affected. For example, if you disable alarms on the default profile, other profiles are unaffected.

Use **alarms** and **no alarms** to enable and disable minor alarms related to DSL subscriber ports. When you disable these alarms, you receive no notification when alarm conditions exist. (Notification methods include console messages, LEDs, the output of the **show facility-alarm status** command, and relay alarm signals to external systems for audible or visible alarms.) However, you can track the condition of DSL ports on which alarms are disabled, including conditions that ordinarily trigger alarms, by using the command **show dsl interface atm** *slot#/port#*.

You can suppress minimum bit rate alarms without disabling other alarms for the profile. See the "cap bitrate" section on page 3-5, and the "dmt bitrate" section on page 3-32.

Note The alarms command has no effect on critical alarms, major alarms, or minor alarms that are related to subsystems other than the DSL subscriber ports.

Examples

In this example, the command enables alarms for the default profile:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile default
DSLAM(cfg-dsl-profile)# alarms
```

Related Commands

Command	Description
dsl profile	Attaches a port to a profile.
show dsl profile	Displays a specific profile and all ports to which the profile is currently attached.
show dsl interface atm *slot#/port#*	Displays DSL, DMT, CAP, and ATM status for a port.
show facility-alarm status	Displays the current major and minor alarm status.

aps clear

To clear outstanding APS priority requests, use the **aps clear** privileged EXEC command.

aps clear *atm interface*

Syntax Description

atm interface	ATM interface for which you want to clear all APS priority requests.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Usage Guidelines

The **aps clear** EXEC command allows you to remove all of the APS priority requests on the named ATM interface.

Note This command works only on SONET interfaces in redundant configurations.

Examples

The following example clears outstanding APS priority requests on interface atm 0/1:

```
DSLAM> enable
DSLAM# aps clear atm 0/1
```

Related Commands

Command	Description
aps force	Force a switchover to the specified fiber regardless of the failure state.
aps lockout	Prevent the protection fiber from being the active fiber and from being switched to by manual, automatic, and forced switchovers.
aps manual	Force a switch to the specified fiber only if the fiber that is being switched to is not in a failed state.
show aps	Display the APS status of each SONET port on both NI-2 cards.
show controllers	Display information on working and protection fibers.

aps force

To force a switchover to the specified fiber regardless of the failure state, use the **aps force** privileged EXEC command. To disable the forced switchover, use the **aps clear** command.

aps force *atm interface* **from [protection | working]**

Syntax Description

atm interface	ATM interface for which you want to force the switchover.
protection	The fiber that is local to the NI-2 card in slot 11.
working	The fiber that is local to the NI-2 card in slot 10.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Usage Guidelines

Force is defined as the second highest APS request priority level. The **aps force** command does not persist over a system restart. The request succeeds if no higher priority request is posted. This command forces a switch to the specified fiber regardless of the failure state of the fiber. See Usage Guidelines in the "show aps" section on page 6-3 for information on request priority levels.

Note The working fiber is local to the NI-2 card in slot 10, and the protection fiber is local to the NI-2 card in slot 11.

Examples

The following example forces a switch on interface ATM 0/2 from the working fiber to the protection fiber:

```
DSLAM> enable
DSLAM# aps force atm 0/2 from working
```

Related Commands

Command	Description
aps clear	Clear outstanding APS priority requests.
aps lockout	Prevent the protection fiber from being the active fiber and from being switched to by manual, automatic, and forced switchovers.
aps manual	Force a switch to the specified fiber only if the fiber to which the system is switching is not in a failed state.

Command	Description
show aps	Display the APS status of each SONET port on both NI-2 cards.
show controllers	Display information on working and protection fibers.

aps lockout

The **aps lockout** privileged EXEC command prevents automatic, manual, and forced APS switchovers from occurring on the specified SONET interface. To disable aps lockout, use the **aps clear** command.

aps lockout *atm interface*

Syntax Description

atm interface	ATM interface for which you want to lockout the switchover.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Usage Guidelines

Lockout is defined as the highest APS request priority level. The **aps lockout** command does not persist over a system restart. If the working fiber is active, then the **aps lockout** command prevents a switchover to the protection fiber. If the protection fiber is active, then the **aps lockout** command prevents a switchover to the working fiber. See Usage Guidelines in the "show aps" section on page 6-3 for information on request priority levels.

Note If the active fiber goes down while the system is under lockout, no switchover occurs to the protection fiber, and data traffic is interrupted until the active fiber connection is restored.

The following example stops the protection fiber from becoming the active fiber by preventing manual, automatic, or forced APS switchovers on interface ATM 0/1:

```
DSLAM> enable
DSLAM# aps lockout atm 0/1
```

Related Commands

Command	Description
aps clear	Clear outstanding APS priority requests.
aps force	Force a switchover to the specified fiber regardless of the failure state.
aps manual	Force a switch to the specified fiber only if the fiber that is being switched to is not in a failed state.
show aps	Display the APS status of each SONET port on both NI-2 cards.
show controllers	Display information on working and protection fibers.

aps manual

To cause a switchover from the specified fiber to a fiber that is not in a failed state, use the **aps manual** privileged EXEC command. To clear the switchover request, use the **aps clear atm** command.

aps manual *atm interface* **from [protection | working]**

Syntax Description

atm interface	ATM interface from which you want to switch.
protection	The fiber that is local to the NI-2 card in slot 11.
working	The fiber that is local to the NI-2 card in slot 10.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Usage Guidelines

Manual is the third highest APS request priority level. The request succeeds if no higher priority request is posted. The **aps manual** command does not persist over a system restart. The atm interface named in the command is the one from which you want to switch. See Usage Guidelines in the "show aps" section on page 6-3 for information on request priority levels.

Examples

The following example forces a switch from the ATM 0/1 working fiber to the ATM 0/1 protection fiber:

```
DSLAM> enable
DSLAM# aps manual atm 0/1 from working
```

Related Commands

Command	Description
aps clear	Clear outstanding APS priority requests.
aps force	Force a switchover to the specified fiber regardless of the failure state.
aps lockout	Prevent the protection fiber from being the active fiber and from being switched to by manual, automatic, and forced switchovers.
show aps	Display the APS status of each SONET port on both NI-2 cards.
show controllers	Display information on working and protection fibers.

atm clp-drop

To enable the clp-drop flag for all ports, and for selected traffic types, use the **atm clp-drop** command.

atm clp-drop [**force**] {**vbr-nrt** | **ubr**} {**off** | **on**}

Syntax Description

[**force**]	Change the clp-drop setting on an active interface, even if the change results in loss of data.
{**vbr-nrt** | **ubr**}	The appropriate traffic parameters.
{**off** | **on**}	Select off to disable the clp-drop flag or on to enable it.

Defaults

Off

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

If the clp-drop flag is enabled, the software drops cells when the specified service-category queues reach 50 percent of the discard threshold limit. This reduces congestion in busy flows.

Examples

In this example, the command enables the clp-drop flag for UBR traffic:

```
DSLAM# configure terminal
DSLAM(config)# atm clp-drop ubr on
```

Related Commands

None

atm connection-traffic-table-row

To create an entry in the traffic characteristics table, use the **atm connection-traffic-table-row** global configuration command. To delete an entry, use the **no** form of this command.

atm connection-traffic-table-row [index *row-index***] [name** *string*] **cbr pcr** *rate* **[cdvt** *cdvt-value***]**

atm connection-traffic-table-row [index *row-index***] [name** *string*] **{vbr-rt | vbr-nrt} pcr** *rate* **{scr0 | scr10}** *scr-value* **[mbs** *mbs-value***] [cdvt** *cdvt-value***]**

atm connection-traffic-table-row [index *row-index***] [name** *string*] **abr pcr** *rate* **[cdvt** *cdvt-value***] [mcr** *mcr-value***]**

atm connection-traffic-table-row [index *row-index***] [name** *string*] **ubr pcr** *rate* **[cdvt** *cdvt-value***] [mcr** *mcr-value***]**

no atm connection-traffic-table-row index *row-index*

Syntax Description

cdvt *cdvt-value*	The value of the cell delay variation tolerance, in the range of 0 to 2147483647, expressed in cell-times (2.72 microseconds at 155.2 Mbps).
mbs *mbs-value*	The value of the maximum burst size, in the range of 0 to 2147483647, expressed in the number of cells.
mcr *mcr-value*	The minimum cell rate is a positive integer, measured in kilobits per second, in the range of 0 to 910533065.
name *string*	A unique identifier, up to 16 characters, for the traffic table row. The name is nvgened to retain the binding across reloads.
pcr *rate*	The peak cell rate is a positive integer, measured in kilobits per second, in the range of 0 to 910533065.
row-index	An integer in the range of 1 to 1073741823.
scr0	Sustained cell rate for the CLP 0 flow.
scr10	Sustained cell rate for the CLP 0+1 flow.
scr-value	The sustained cell rate is a positive integer, measured in kilobits per second in the range of 0 to 910533065.

Defaults

Rows 1 through 6 in the table are predefined.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.2(7)DA	The **name** keyword was introduced.

Usage Guidelines

This command sets up the traffic characteristics used in PVC, PVP, soft-vc, and soft-vp definition. The characteristics are stored as rows of a table. To reference a row index when you create a PVC, use the **atm pvc** command in interface configuration mode. To reference a row index when you create a PVP, use the **atm pvp** command. To reference row indexes when you create a soft-vc or soft-vp, use the **atm soft-vc** command and **atm soft-vp** command, respectively.

When you use the **atm connection-traffic-table-row** command without the index clause, the software uses a free-row index, which is displayed if the command is successful.

When the CDVT or MBS parameter is not specified in the creation of a row, the software chooses a configurable interface default value to use in UPC.

Six connection traffic table rows are defined by default and are numbered 1 through 6. Row 1 is the default row used by the **atm pvc** command if no rows are explicitly specified. Use the **show atm connection-traffic-table** command to display the default configurations for rows 2 through 6.

You cannot delete default rows.

Row 1 PCR represents the maximum cell rate that fits in 24 bits.

When you configure an ABR row and do not specify MCR, the software configures MCR as 0 in the CTT row.

The default rows do not have any names.

Examples

In the following example, a CBR CTT row is defined with an index of 200 and a peak cell rate of 7743 kbps.

```
DSLAM(config)# atm connection-traffic-table-row index 200 name traffic-row1 cbr pcr 7743
```

Related Commands

Command	Description
atm pvc	Creates a PVC.
atm pvp	Creates a PVP.
atm soft-vc	Creates a soft PVC on a DSLAM.
atm soft-vp	Creates a soft PVP on a DSLAM.
show atm connection-traffic-table	Displays entries in the traffic characteristics table.

atm input-queue

To change the maximum size of the input queue for each subscriber port, use the **atm input-queue** interface configuration command. To reset the maximum queue size to the default value, use the **no** form of the command.

atm input-queue [**force**] {**cbr | vbr-rt | vbr-nrt | ubr**} **max-size** *size-num*

no atm input-queue [**force**] {**cbr | vbr-rt | vbr-nrt | ubr**} **max-size**

Syntax Description

[force]	Change the input queue size on an active interface, even if the change results in the loss of data from the queue.
{cbr | vbr-rt | vbr-nrt | ubr}	Select the appropriate traffic parameter.
max-size *size-num*	Maximum input queue size per service category. Enter queue size in cells, from 8 to 262144. If you enter a value that is not a power of 2, the system rounds up or down to the nearest power of 2 and uses that value. For example, if you enter 14, the system rounds up to 16.

Defaults

The defaults vary by queue (traffic type) as shown here:

cbr	vbr-rt	vbr-nrt	ubr
1024 cells	1024 cells	8192 cells	8192 cells

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced in a previous release. The range of queue sizes and the type of port affected by the command were changed for Release 12.0(5)DA.

Usage Guidelines

This command is supported only on subscriber ports.

The **force** argument indicates that the change will be made even if it results in the loss of data on the interface queue (the queue must be momentarily disabled for the threshold to be changed). This command without the **force** argument changes the threshold only if the interface is down. An error message appears and the command does not take effect if the interface is up and the **force** argument is not present.

To display both the configured and installed values of *size-num*, use the **show atm interface resource** command.

Examples

In the following example, the maximum size of the vbr-nrt input queue is set to 512 cells. You can set this even if the interface is up.

```
DSLAM(config-if)# atm input-queue force vbr-nrt max-size 512
```

Related Commands

Command	Description
atm input-threshold	Sets input queue discard threshold values.
show atm interface	Displays ATM-specific information about all ATM interfaces.
show atm interface resource	Displays resource management interface configuration status and statistics.

atm input-threshold

To set input-queue discard-threshold values for this node and for any subtended nodes subordinate to this node, use the **atm input-threshold** global configuration command. To reset a threshold to its default value, use the **no** form of the command.

atm input-threshold {**cbr** | **vbr-rt** | **vbr-nrt** | **ubr**} {**epd** *threshold-value* | **drop** *threshold-value*}

no atm input-threshold {**cbr** | **vbr-rt** | **vbr-nrt** | **ubr**} {**epd** | **drop**}

Syntax Description

{**cbr** | **vbr-nrt** |**vbr-rt** | **ubr**}	Select the traffic priority. Threshold settings apply to all queues of a given priority.
epd	Early packet discard threshold. The **epd** value plus the **drop** value equals the total size of the input queue. For details, see the Usage Guidelines.
drop	Drop threshold. The **drop** value plus the **epd** value equals the total size of the input queue. For details, see Usage Guidelines.
threshold-value	Enter the allowed maximum input discard threshold, in cells, for subscriber and subtending ports for the selected traffic parameter. The range is 8 to 262144. If you enter a value that is not a power of 2, the system rounds up or down to the nearest power of 2 and uses that value. For example, if you enter 18, the system rounds down to 16. If you enter a value that falls halfway between two powers of 2, the system rounds up. For example, if you enter 12, the system rounds up to 16.

Defaults

The defaults vary by interface type and by traffic priority, as shown here:

		Number of Cells			
Interface	**Queue Segment**	**cbr**	**vbr-rt**	**vbr-nrt**	**ubr**
DS3	**epd**	512	512	4096	4096
	drop	512	512	4096	4096
	Total queue	1024	1024	8192	8192
OC-3c	**epd**	2048	2048	8192	8192
	drop	2048	2048	8192	8192
	Total queue	4096	4096	16384	16384
T1/E1	**epd**	512	1024	2048	2048
	drop	512	1024	2048	2048
	Total queue	1024	2048	4096	4096

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

We recommend that you leave the input queue discard thresholds set to their default values, which are adequate for most configurations.

This command controls the discard threshold settings for up to 52 input queues—one queue for each of four traffic types on each of up to 13 nodes in a subtending group. The behavior of the input queues is affected not only by the input queue discard threshold settings, but also by the setting of the intelligent packet discard feature, which is controlled with the **atm pvc** command and the **atm soft-vc** command. The packet discharge setting determines whether the system performs packet-based discards or cell-based discards:

- When packet discharge is enabled, the system performs packet-based discards—that is, when discarding is triggered, the system drops data from the first cell dropped, up to the end of the current AAL5 packet.

  This discard method includes policer and partial packet discard (PPD) drops, or entire AAL5 packets (for early packet discard (EPD) drops). The system accepts or rejects subsequent data on a packet-by-packet basis.

- When packet discharge is disabled, the system performs cell-based discards—that is, when discarding, the system drops a cell at a time, and accepts or rejects subsequent data on a cell-by-cell basis. Cell-based discarding is the default behavior.

The packet discharge setting applies to all discards, whether for reasons of queue exhaustion or policing. Packet discharge is disabled by default; use the commands **atm pvc** *vpi vci* **pd** {**on** | **off**} or **atm soft-vc** *vpi vci* **pd** { **on** | **off** } to enable or disable it.

The input queue discard thresholds work as follows:

- If packet-based discard is in force (the packet discharge feature is enabled), the input queue absorbs packets until the queue reaches the **epd** threshold. At that point, the queue absorbs the remainder of the current packet, as long as doing so does not cause the queue to fill completely. (The total queue size equals **epd** value plus **drop** value.)

  After it reaches the **epd** threshold, the queue drops all subsequent packets until the queue contents drop below the **epd** threshold. If the queue fills completely before the current packet finishes, then PPD occurs.

- If cell-based discard is in force (the packet discharge feature is disabled), add the **epd** and **drop** threshold values to determine the input queue size. When the queue is full, it drops all subsequent cells until its contents fall below the combined threshold value.

If packet-based discard is in force, you can implicitly configure the input queue discard thresholds for either EPD or PPD. For EPD, configure a **drop** threshold value that is large enough to allow most packets to enter the queue. Appropriate values for this purpose vary by traffic type, but see the thresholds in the *Defaults* section for examples of EPD settings. For PPD, configure a small **drop** threshold value. This forces the system to discard the remainder of the packet that fills up the queue.

To set input queue sizes, use the **atm input-queue** command.

Examples

In this example, the command sets the **epd** threshold for CBR traffic on subscriber and subtending ports at 32,000 cells:

```
DSLAM# configure terminal
DSLAM(config)# atm input-threshold cbr epd 32000
```

Related Commands

Command	Description
atm input-queue	Changes the maximum size of the input queue for each subscriber port.
atm output-threshold	Changes the output queue discard thresholds for the subscriber ports.
atm pvc *vpi vci* **pd** {**on** | **off**}	Creates a PVC on a subscriber port.

atm ni2-switch trunk

To select the interface to use as the trunk on a DS3/8xT1 card, use the **atm ni2-switch trunk** command. To reset this command to the default value, use the **no** form of this command.

atm ni2-switch trunk {atm0/1 | atm0/2 | atm0/3 | atm0/4 | atm0/5 | atm0/6 | atm0/7 | atm0/8 | atm0/9 | atm0/ima0 | atm0/ima1 | atm0/ima2 | atm0/ima3}

Syntax Description

{atm0/1 | atm0/2 | atm0/3 | atm0/4 | atm0/5 | atm0/6 | atm0/7 | atm0/8 | atm0/9 | atm0/ima0 | atm0/ima1 | atm0/ima2 | atm0/ima3}	The interface to use as the trunk.

Defaults

The DS3 link is the default trunk interface on the DS3+T1 I/O module (**atm ni2-switch trunk atm0/1**).

The first E1 link (atm0/2) is the default trunk interface on the E1 I/O module (**atm ni2-switch trunk atm0/2**).

Note Before you reassign trunk status from an active link or IMA group to a different link or IMA group, you must administratively shut down both the current trunk and the interface to be assigned trunk status.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

Table 2-3 provides the trunk interface and the name to use for it in this command.

Table 2-3 Interface Name for Trunk

Trunk	Interface Name
DS3 link	atm 0/1
T1/E1 link 0	atm 0/2
T1/E1 link 1	atm 0/3
T1/E1 link 2	atm 0/4
T1/E1 link 3	atm 0/5

Table 2-3 Interface Name for Trunk (continued)

Trunk	Interface Name
T1/E1 link 4	atm 0/6
T1/E1 link 5	atm 0/7
T1/E1 link 6	atm 0/8
T1/E1 link 7	atm 0/9
IMA group 0	atm 0/ima0
IMA group 1	atm 0/ima1
IMA group 2	atm 0/ima2
IMA group 3	atm 0/ima3

Examples

In the following example, the trunk interface is set to T1/E1 link 2.

```
DSLAM(config)# interface atm0/3
DSLAM(config-if)# shutdown
DSLAM(config)# atm ni2-switch trunk atm0/4
```

Related Commands

Command	Description
show atm interface	Displays ATM-specific information about all ATM interfaces.

atm oam intercept segment

The **atm oam intercept segment** command is a global configuration command that enables the NI-2 to accept ATM OAM segment cells on "up" atm connections. If a connection is down, ATM OAM segment cells are not received. The command is enabled by default. Use the **no** form to disable the NI-2 from receiving ATM OAM segment cells

atm oam intercept segment

no oam intercept segment

Syntax Description

This command has no arguments or keywords.

Defaults

The command is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(10)DA	This command was introduced.

Usage Guidelines

You can determine the state of this setting by using the **show running-config** command to check for **no atm oam intercept segment**. The default setting, **atm oam intercept segment**, is not displayed by **show running-config**.

Examples

In this example, the reception of ATM OAM segment cells by NI-2 is disabled.

```
DSLAM# configure terminal
DSLAM(config)# no atm oam intercept segment
```

Related Commands

Command	Description
atm oam intercept end-to-end	Enable/disable accepting ATM end-to-end OAM cells. For more information, see http://www.cisco.com/univercd/cc/td/doc/product/atm/c8540/12_1/12_c_e/command/atm.htm#xtocid71.

atm output-threshold

To change the output queue discard thresholds for the subscriber ports, use the **atm output-threshold** interface configuration command. To reset a threshold to its default value, use the **no** form of the command.

atm output-threshold {**cbr** | **vbr-rt** | **vbr-nrt** | **ubr**} {**epd** *threshold-value* | **drop** *threshold-value*}

no atm output-threshold {**cbr** | **vbr-rt** | **vbr-nrt** | **ubr**} {**epd** | **drop**}

Syntax Description

{**cbr** | **vbr-rt** | **vbr-nrt** | **ubr**}	Traffic priority. Threshold settings apply to all queues of a given priority.
epd	Early packet discard threshold. The **epd** value plus the **drop** value equals the total size of the output queue. For details, see the Usage Guidelines section.
drop	Drop threshold. The **drop** value plus the **epd** value equals the total size of the output queue. For details, see the Usage Guidelines section.
threshold-value	Enter the allowed maximum output discard threshold, in number of cells, for subscriber ports for the selected traffic parameter. The range is 8 to 262144. If you enter a value that is not a power of 2, the system rounds up or down to the nearest power of 2 and uses that value. For example, if you enter 18, the system rounds down to 16. If you enter a value that falls halfway between two powers of 2, the system rounds up. For example, if you enter 12, the system rounds up to 16.

The defaults vary by traffic priority, as shown here:

	Number of Cells			
Queue Segment	**cbr**	**vbr-rt**	**vbr-nrt**	**ubr**
epd	128	128	1024	1024
drop	128	128	1024	1024
Total queue	256	256	2048	2048

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

We recommend that you leave the output queue discard thresholds set to their default values, which are adequate for most configurations.

The **atm output-threshold** command controls the discard threshold settings for up to 1040 output queues. The behavior of the output queue is controlled not only by the output queue discard threshold settings, but also by the setting of the intelligent packet discard feature, which is controlled with the **atm pvc** command.

The packet discharge setting determines whether the system performs packet-based discards or cell-based discards:

- When packet discharge is enabled, the system performs packet-based discards—that is, when discarding is triggered, the system drops data from the first cell dropped, up to the end of the current AAL5 packet.

  This discard method includes policer and PPD drops, or entire AAL5 packets (for EPD drops). The system accepts or rejects subsequent data on a packet-by-packet basis.

- When packet discharge is disabled, the system performs cell-based discards—that is, when discarding, the system drops a cell at a time, and accepts or rejects subsequent data on a cell-by-cell basis. Cell-based discarding is the default behavior.

The packet discharge setting applies to all discards, whether the discards occur for reasons of queue exhaustion or policing. Packet discharge is disabled by default; use the command **atm pvc** *vpi vci* **pd** {**on** | **off**} to enable or disable it.

The output queue discard thresholds work as follows:

- If packet-based discard is in force (the packet discharge feature is enabled), the output queue absorbs packets until the queue reaches the **epd** threshold. At that point, the queue absorbs the remainder of the current packet, as long as doing so does not cause the queue to fill completely. (The total queue size equals **epd** value plus **drop** value.)

  After it reaches the **epd** threshold, the queue drops all subsequent packets until the queue contents drop below the **epd** threshold. If the queue fills completely before the current packet finishes, then PPD occurs.

- If cell-based discard is in force (the packet discharge feature is disabled), add the **epd** and **drop** threshold values to determine the output queue size. When the queue is full, it drops all subsequent cells until its contents fall below the combined threshold value.

If packet-based discard is in force, you can implicitly configure the output queue discard thresholds for either EPD or PPD. For EPD, configure a **drop** threshold value that is large enough to allow most packets to enter the queue. Appropriate values for this purpose vary by traffic type; see the thresholds in the Defaults section for examples of EPD settings. For PPD, configure a very small **drop** threshold value to force the system to discard the remainder of the packet that fills up the queue.

Examples

In this example, the command sets the **drop** threshold for VBR-NRT traffic on subscriber ports at 16,000 cells:

```
DSLAM# configure terminal
DSLAM(config)# interface atm0/1
DSLAM(config-if)# atm output-threshold vbr-nrt drop 16000
```

Related Commands

Command	Description
atm input-threshold	Sets input queue discard threshold values.
show atm interface resource	Displays resource management interface configuration status and statistics.
atm pvc *vpi vci* **pd** {**on** | **off**}	Creates a PVC on a subscriber port.

atm pvc

To create a PVC, use the **atm pvc** interface configuration command. To create a permanent virtual channel connection (PVCC), use the long form of the **atm pvc** command. To create a permanent virtual channel link (PVCL), use the short form of the **atm pvc** command. To remove the specified PVC, use the **no** form of this command.

atm pvc *vpi-A* [*vci-A* | **any-vci**] [**upc** *upc-A*] [**pd** *pd*] [**rx-cttr** *index*] [**tx-cttr** *index*] **interface atm** *slot-B/port-B vpi-B* [*vci-B* | **any-vci**] [**upc** *upc-B*] [**name** *string*] [**conn-type** *conntype-B*]

atm pvc *vpi vci* [**upc** *upc*] [**pd** *pd*] [**rx-cttr** *index*] [**tx-cttr** *index*]

no atm pvc *vpi vci*

Note The A and B suffixes of the command arguments refer to the ends of the connection. A is the local end; B is the remote end.

Syntax Description

vpi — Virtual path identifier of this PVC. On the route processor port (ASP) interface, ATM0/0, the VPI is always 0. On DSL interfaces, the VPI range is 0 to 255. The VPI is an 8-bit field in the header of the ATM cell. The VPI value is unique only on an interface, not throughout the ATM network (the VPI has local significance only).

For information on assigning VPIs to shaped VP tunnels, see the Usage Guidelines section.

vci — VCI of this PVC. The range of values varies by interface type, mode, and VPI, as shown below.

The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single interface, not throughout the ATM network (it has local significance only).

ASP Interface (ATM0/0)	VCI Range
	32 to 4095

DSL Interfaces	VCI Range
In manual-well-known-vc mode	
VPI = 0	1 to 255
VPI other than 0	0 to 255
Not in manual-well-known-vc mode	32 to 255

Other Interfaces	VCI Range
In manual-well-known-vc mode	5 to 16383
In other modes	32 to 16383

any-vci — Selects any available VCI. This feature applies only to the ASP interface (ATM0/0).

upc — Usage parameter control, specified as **pass**, **tag**, or **drop**; the default is **pass**. You can set the *upc* parameter to **tag** or **drop** only on an ATM interface that is not the ASP port (ATM0/0) or a logical port (VP tunnel).

pd — Turns the intelligent packet discard option on or off. The default is off.

rx-cttr *index*	Connection traffic table row index in the received direction. Configure the connection traffic table row before you use the **atm pvc** command. See the **atm connection-traffic-table-row** command for information on configuring the **rx-cttr** parameter. The default is 1.
tx-cttr *index*	Connection traffic table row index in the transmitted direction. Configure the connection traffic table row before you use the **atm pvc** command. See the **atm connection-traffic-table-row** command for information on configuring the **tx-cttr** parameter. The default is 1.
slot#/port#	Slot and port number for the ATM interface.
name *string*	A unique identifier, up to 16 characters, for the PVC connection. The name is unique per DSLAM for all connections. The name is nvgened to retain the binding across reloads.
conn-type	Represents the PVC type for this connection with values local or end-to-end. The default value is local. Used by the management stations to distinguish the connections on a subtend path.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.2(5)DA	The **name** keyword was introduced.
12.2(7)DA	The **conn-type** keyword was introduced.

Usage Guidelines

Use the **atm pvc** commands to create or delete the following types of ATM connections:

- Transit point-to-point PVCC
- Point-to-point PVCL
- Point-to-point permanent virtual channel connection terminated at ASP (terminating VC)

When you set UBR connections, the tx-cttr and rx-cttr fields are not needed. However, these fields are required when you set up a CBR, VBR, or ABR connection. See the "atm connection-traffic-table-row" section on page 2-19 for information on creating an entry in the traffic characteristics table.

Assigning VPI Values to Shaped VP Tunnels

If you configure VP tunnels with traffic shaping, you can use only 32 VPIs, even though the full range of VPI values is 0 to 255. If you have not yet assigned any VPIs, all values from 0 to 255 are available. Once you begin to assign VPIs, however, the assigned VPIs limit the VPIs that remain. (You assign VPIs by using the **atm pvp** or **atm pvc** commands.)

After a particular VPI value is assigned to a shaped VP tunnel, every 32nd VPI value above and below the first one is eliminated—that is, the original value modulo 32. For example, if you assign VPI 94 to a shaped VP tunnel, the following VPI values become unavailable for any purpose: 30, 62, 126, 158, 190, and 222.

To avoid problems, choose a block of 32 consecutive VPI values (for example, 0 to 31 or 101 to 132). The software rejects invalid VPI values.

Examples

The following example shows how to configure a terminating PVC between interface ATM 3/1 and the ASP port (ATM 0/0).

```
DSLAM(config)# interface atm 0/0
DSLAM(config-if)# atm pvc 0 any-vci interface atm 3/1 0 100
```

The following example shows how to set up a UBR PVC connection between interface ATM 4/1 and ATM 4/,2 with VPI 0 and VCI 40.

```
DSLAM(config)# interface atm 4/1
DSLAM(config-if)# atm pvc 0 40 interface atm 4/2 0 40
```

The following example shows a display using the encap variable.

```
DSLAM(config-if)# atm pvc 100 200 interface atm 0/0 0 344 encap ?
aal5mux   AAL5+MUX Encapsulation
aal5snap AAL5+LLC/SNAP Encapsulation
```

The following example shows the commands that you use to establish a PVC between a logical interface (VP tunnel) on ATM 4/1.99 and ATM 3/1.

```
DSLAM(config)# interface atm 4/1.99
DSLAM(config-subif)# atm pvc 99 100 interface atm 3/1 0 89
DSLAM(config-subif)# end
```

The following example shows how to use the **show atm vc** command to display all VCs on an interface.

```
DSLAM# show atm vc interface atm 0/1.51
Interface  VPI   VCI   Type   X-Interface  X-VPI X-VCI  Status   Name
ATM0/1.51  51    3      PVC     ATM0/0     0     75     DOWN
ATM0/1.51  51    4      PVC     ATM0/0     0     76     DOWN
ATM0/1.51  51    5      PVC     ATM0/0     0     74     DOWN
ATM0/1.51  51    16     PVC     ATM0/0     0     73     DOWN
```

The following example deletes a previously configured ATM transit point-to-point PVC.

```
DSLAM(config-if)# interface atm 1/1
DSLAM(config-if)# no atm pvc 50 100
```

Related Commands

Command	Description
atm connection-traffic-table-row	Creates an entry in the traffic characteristics table.
atm pvp	Creates a PVP on a subscriber port.
show atm interface	Displays ATM-specific information about all ATM interfaces.
show atm vc	Displays the ATM layer connection information about the virtual connection.

atm pvp

To create a permanent virtual path (PVP), use the **atm pvp** interface configuration command. To create a permanent virtual path connection (PVPC), use the long form of the **atm pvp** command. To create a permanent virtual path link (PVPL), use the short form of the **atm pvp** command. To remove the specified PVP, use the **no** form of this command.

atm pvp *vpi-A* [**cast-type** *type-A*] [**upc** *upc-A*] [**rx-cttr** *index*] [**tx-cttr** *index*]
interface atm *slot#/port#* [**cast-type** *type-B*] [**upc** *upc-B*] [**name** *string*][**conn-type** *conntype-B*]

atm pvp *vpi* [**cast-type** *type*] [**hierarchical** | **shaped**] [**upc** *upc*] [**rx-cttr** *index*] [**tx-cttr** *index*]

no atm pvp *vpi*

Syntax Description

vpi	The VPI value is unique only on a single interface, not throughout the ATM network (it has local significance only).
type	Specified as **p2p**, **p2mp-root**, or **p2mp-leaf**. The default is **p2p**.
upc	Usage parameter control, specified as **pass**, **tag**, or **drop**. The default is **pass**. The *upc* variable can be set to **tag** or **drop** only under the following conditions: • The ATM interface is not the route processor port (ATM 0) or a logical port (VP tunnel). • The connection is not the leaf of a point-to-multipoint connection.
rx-cttr	Connection traffic table row index in the received direction. Configure the connection traffic table row before you use the **atm pvc** command. See the **atm connection-traffic-table-row** command for information on configuring the **rx-cttr** parameter. The default is 1.
shaped	The PVP is a VP tunnel that should use hardware shaping of the aggregate transmit flow of cells. Only CBR PVPs can be shaped VP tunnels. **Note** Hierarchical tunnels are not supported on DSLAM platform hardware.
tx-cttr	Connection traffic table row index in the transmitted direction. The connection traffic table row should be configured before using **atm pvc** command. See the **atm connection-traffic-table-row** command for information on configuring the **tx-cttr** parameter. The default is 1.
slot#/port#	Slot and port number for the ATM interface.
name *string*	A unique identifier, up to 16 characters, for the PVP connection. The name is unique per DSLAM for all connections. The name is nvgened to retain the binding across reloads.
conn-type	Represents the PVP type for this connection with values local or end-to-end. The default value is local. Used by the management stations to distinguish the connections on a subtend path.

Defaults

See Syntax Description.

Command Modes Interface configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.2(7)DA	The **name** keyword was introduced.
12.2(7)DA	The **conn-type** keyword was introduced.

Usage Guidelines When you specify the PVP as shaped, you must subsequently use it as a VP tunnel (by the **interface** command). You can use only CBR VPs for shaped tunnels. A shaped PVP cannot be cross-connected.

Note Hierarchical tunnels are not supported on DSLAM platform hardware.

The commands are used to create or delete the following types of ATM connections on a switch:

- Transit point-to-point PVPC
- Transit point-to-multipoint PVPC
- Point-to-point PVPL
- Point-to-multipoint PVPL

Examples The following example shows a typical configuration for PPP over ATM, using a RADIUS authentication server:

```
DSLAM(config)# interface virtual-template 1
DSLAM(config-if)# ip unnumbered ethernet 0/0
DSLAM(config-if)# peer default ip address pool telecommuters
DSLAM(config-if)# ppp authentication chap
DSLAM(config-if)# exit
DSLAM(config)# ip local pool telecommuters 10.36.1.1 10.36.1.254

DSLAM(config)# aaa new-model
DSLAM(config)# aaa authentication ppp default radius
DSLAM(config)# radius-server host 172.31.5.96
DSLAM(config)# radius-server key foo
DSLAM(config)# radius-server attribute nas-port format e

DSLAM(config)# interface atm 1/1
DSLAM(config-if)# atm pvp 1
DSLAM(config-if)# interface atm 1/1.40 multipoint
DSLAM(config-subif)# pvc 0/50
DSLAM(config-if-atm-vc)# encapsulation aal5mux ppp virtual-template 1
DSLAM(config-if-atm-vc)# exit
DSLAM(config-subif)# pvc 0/51
DSLAM(config-if-atm-vc)# encapsulation aal5mux ppp virtual-template 1
DSLAM(config-if-atm-vc)# exit
```

Related Commands

Command	Description
atm connection-traffic-table-row	Creates an entry in the traffic characteristics table.
atm pvc	Creates a PVC on a subscriber port.
show atm interface	Displays ATM-specific information about all ATM interfaces.
show atm vp	Displays the ATM layer connection information about the virtual path.

atm route-bridged

To configure an interface to use ATM route-bridged encapsulation, use the **atm route-bridged** interface configuration command.

atm route-bridged ip

Syntax Description

ip	Route IP over RFC 1483 Ethernet.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Examples

The following example configures ATM route-bridge encapsulation on an interface:

```
DSLAM(config)# interface atm 1/1
DSLAM(config-if)# ip address 172.69.5.9 255.255.255.0
DSLAM(config-if)# atm route-bridged ip
DSLAM(config-if)# pvc 0/32
```

atm soft-vc

To create a soft PVC on the DSLAM, use the **atm soft-vc** interface configuration command.

atm soft-vc *source-vpi source-vci* **dest-address** *atm-address dest-vpi dest-vci* [**enable** | **disable**] [**upc** *upc*] [**pd** *pd*] [**rx-cttr** *index*] [**tx-cttr** *index*] [**retry-interval** [**first** *retry-interval*] [**maximum** *retry-interval*]] [**explicit-path** *precedence* {**name** *path-name* | **identifier** *path-id*} [**upto** *partial-entry-index*] [*only-explicit*]] **[name** *string*]

For existing soft PVCs, use the **no** form of the command to delete the soft PVC.

no atm soft-vc *source-vpi source-vci*

To respecify the explicit paths, use the **redo-explicit** form.

atm soft-vc *source-vpi source-vci* [**enable** | **disable**] [**redo-explicit** [**explicit-path** *precedence* **{name** *path-name* | **identifier** *path-id*} [**upto** *partial-entry index*] [*only-explicit*]]]

To signal connections with nonstandard user-defined traffic management options, use the alternate-signalling tagging form. This form may be beneficial in networks where switches use these options to manage UPC options in a manner other than that currently defined by PNNI.

atm soft-vc alternate-signalling tagging {*fwd* **|** *bwd* **|** *bidir***}**

Syntax Description

source-vpi	Source VPI number.
source-vci	Source VCI number.
dest-address *atm-address*	ATM address for the destination port.
dest-vpi	Destination VPI number.
dest-vci	Destination VCI number.
enable	Allows the soft connection to be set up; **enable** is the default for the initial soft connection configuration. **Note** If you enter the **soft-connection** command for an existing connection, the default is the current enabled or disabled state.
disable	Prevents an initial soft connection from being set up, or tears down an existing connection.
upc *upc*	Usage parameter control, specified as **pass** | **tag** | **drop**; the default is **pass**. You can set the **upc** option to **tag** or **drop** only when the connection is not the leaf of a point-to-multipoint connection.
pd *pd*	Intelligent packet discard option, specified as **on** | **off**. The default is **off**.
rx-cttr *index*	Connection traffic table row index in the received direction. You should configure the **cttr** before you use the **atm pvc** command. See the **atm connection-traffic-table-row** command for information on configuring the **rx-cttr**. The default is 1.
tx-cttr *index*	Connection traffic table row index in the transmitted direction. You should configure the **cttr** before you use the **atm pvc** command. See the **atm connection-traffic-table-row** command for information on configuring the **tx-cttr**. The default is 1.

retry-interval	Configures the retry interval timers for a soft PVC.
first *retry-interval*	Retry interval for the first retry after the first failed attempt, specified in milliseconds. If the first retry after the first failed attempt also fails, the subsequent attempts are made at intervals computed using the **first** *retry-interval* as follows: (2 ** (*k*-1)) * **first** *retry-interval* Where the value of *k* is 1 for the first retry after the first failed attempt and is incremented by 1 for every subsequent attempt. Range is from 100 to 3600000 milliseconds; the default is 5000 milliseconds.
maximum *retry-interval*	The maximum retry interval between any two attempts, specified in seconds. Once the retry interval is computed in the **first** *retry-interval* and becomes equal to or greater than the **maximum** *retry-interval* configured, the subsequent retries will be done at regular intervals of **maximum** *retry-interval* seconds until the call is established. Range is from 1 to 65535 seconds; the default is 60.
redo-explicit	Applies only to existing soft connections and allows you to respecify explicit paths without tearing down connections. Existing connections are unaffected unless a reroute takes place, and then they use the newer **explicit-path** configuration.
explicit-path	The PNNI explicit path that is manually configured for routing a soft PVC, using the **atm pnni explicit-path** command.
precedence	The precedence number by which ATM PNNI explicit paths are assigned, from 1 to 3. You can assign up to three explicit paths to a soft PVC.
name *path-name*	The name of the ATM PNNI explicit path for routing soft PVCs.
identifier *path-id*	Specifies the path ID for the explicit path being configured to route soft PVCs.
upto *partial-entry-index*	Allows the use of a subset of a longer explicit path, so that all included nodes after the specified entry index are disregarded. If the destination is reachable at any next node or segment target, the remaining included nodes in the explicit path are disregarded automatically.
only-explicit	If you specified one or more explicit paths and if the explicit path fails, the soft connection remains down until it is retried at its next retry interval. If you do not specify this option, the system uses the standard on-demand routing instead of waiting for the next retry interval.
name *string*	A unique identifier, up to 16 characters, for the soft PVC connection. The name is unique per DSLAM for all connections. The name is nvgened to retain the binding across reloads.
alternate-signalling tagging	Allows signal connections with nonstandard user-defined traffic management options. You must set the **upc** option tag.
bidir	Signals both the forward and backward tagging options if UPC tagging is configured for a soft PVC on this interface.

bwd	Signals only the backward tagging option if UPC tagging is configured for a soft PVC on this interface.
fwd	Signals only the forward tagging option if UPC tagging is configured for a soft PVC on this interface.

Defaults

See Syntax Description.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.2(5)DA	The **name** and **alternate-signalling tagging** keywords were added.

Usage Guidelines

Obtain the destination port address before configuring a soft PVC by using the **show atm interface** or **show atm addresses** command on the destination DSLAM**.**

The creation of a soft PVC might be unsuccessful because of the following scenarios:

- A VPI or VCI collision at the source or destination DSLAM.
- The source or destination interface is not up (or autoconfiguration is not complete).
- The specified destination address is incorrect.

You can assign up to three explicit paths to a soft VC, by using precedence numbers 1 through 3. The system considers the precedence 1 explicit path as the primary path and tries it first. If it fails, the next precedence path is tried. You can specify explicit paths either by **name** or by **identifier**.

You can change the explicit path options without tearing down an existing soft PVC. Use the **redo-explicit** form of the command to respecify all of the explicit path options.

After configuring a soft PVC, use the **show atm vc interface** command on the source node (specify the source VPI and source VCI) to verify that the soft PVC is working and to see the explicit path that the software is using.

Note The configuration that displays for soft connections with explicit paths is always shown as two separate lines. The **redo-explicit** keyword is on the second line, even if it was originally configured through the use of a single command line.

Note To use the **atm soft-vc alternate-signalling tagging** command, you must shut down the interface and set the **upc** to **tag**.

Examples

The following example shows how a user at the destination DSLAM displays the address of the destination port.

```
DSLAM> show atm address

Switch Address(es):
  47.0091.8100.0000.0005.312a.2c01.0005.312a.2c01.00 active
  NOTE: Switch addresses with selector bytes 01 through 7F
        are reserved for use by PNNI routing

PNNI Local Node Address(es):
  47.0091.8100.0000.0005.312a.2c01.0005.312a.2c01.01 Node 1

Soft VC Address(es):
  47.0091.8100.0000.0005.312a.2c01.4000.0c98.0010.00 ATM0/1
  47.0091.8100.0000.0005.312a.2c01.4000.0c98.0020.00 ATM0/2
  47.0091.8100.0000.0005.312a.2c01.4000.0c98.0030.00 ATM0/3
  47.0091.8100.0000.0005.312a.2c01.4000.0c98.0040.00 ATM0/4
  47.0091.8100.0000.0005.312a.2c01.4000.0c98.0050.00 ATM0/5
  47.0091.8100.0000.0005.312a.2c01.4000.0c98.0060.00 ATM0/6
  47.0091.8100.0000.0005.312a.2c01.4000.0c98.0070.00 ATM0/7
  47.0091.8100.0000.0005.312a.2c01.4000.0c98.0080.00 ATM0/8
  47.0091.8100.0000.0005.312a.2c01.4000.0c98.0090.00 ATM0/9
  47.0091.8100.0000.0005.312a.2c01.4000.0c90.00a0.00 ATM0/IMA0
  47.0091.8100.0000.0005.312a.2c01.4000.0c90.00b0.00 ATM0/IMA1
  47.0091.8100.0000.0005.312a.2c01.4000.0c90.00c0.00 ATM0/IMA2
  47.0091.8100.0000.0005.312a.2c01.4000.0c90.00d0.00 ATM0/IMA3
```

The following example shows how to configure a soft-vc with the alternative tagging option set to forward.

```
DSLAM(config)# interface atm 0/1
DSLAM(config-if)# atm soft-vc alternate-signalling tagging fwd
```

Related Commands

Command	Description
atm pnni explicit-path	Creates or modifies PNNI explicit paths.
show atm addresses	Displays the active ATM addresses on a switch.
show atm vc	Displays all ATM virtual circuits (PVCs and SVCs) and traffic information.

atm soft-vp

To create a soft PVP on the DSLAM, use the atm soft-vp interface configuration command.

atm soft-vp *vpi-s* **dest-address** *address vpi-d* **[upc** ***up*****c] [rx-cttr** ***inde*****x] [tx-cttr** ***inde*****x]**
[retry-interval [first ***retry-interva*****l] [maximum** *retry-interva*l**][name** *string***]**

For existing soft PVPs, use the **no** form of the command to delete the soft PVP.

no atm soft-vp ***vpi-s***

Use the **redo-explicit** form of the command to respecify explicit paths.

atm soft-vp *vpi-s [enable | disable]*
redo-explicit [explicit-path precedence {name path-name | identifier path-id}
[upto **partial-entry-index**] [**only-explicit**]**]**

Syntax Description*[*

source-vpi	Source VPI number.
dest-address *address*	ATM address for the destination port.
vpi-d	Destination VPI number.
upc *upc*	Usage parameter control, specified as **pass** | **tag** | **drop**; the default is **pass**. The **upc** option can be set to **tag** or **drop** only under the following conditions: • The ATM interface is not the route processor port (ATM 0) or a logical port (VP tunnel). • The connection is not the leaf of a point-to-multipoint connection.
rx-cttr *index*	Connection traffic table row index in the received direction. The **cttr** should be configured before you use the **atm soft-vp** command. See the **atm connection-traffic-table-row** command for information on configuring the **rx-cttr**. The default is 1.
tx-cttr *index*	Connection traffic table row index in the transmitted direction. The **ctt** should be configured before you use the **atm soft-vp** command. See the **atm connection-traffic-table-row** command for information on configuring the **tx-ctt**r. The default is 1.
retry-interval	Configures the retry interval timers for a soft VP.
first *retry-interval*	Retry interval for the first retry after the first failed attempt, specified in milliseconds. If the first retry after the first failed attempt also fails, the subsequent attempts are made at intervals computed through the use of the **first** *retry-interval* as follows: (2 ** (*k*-1)) * **first** *retry-interval* Where the value of *k* is 1 for the first retry after the first failed attempt and is incremented by 1 for every subsequent attempt. Range is from 100 to 3600000 milliseconds; the default is 5000 milliseconds.

maximum *retry-interval*	The maximum retry interval between any two attempts, specified in seconds. Once the retry interval is computed in the **first** *retry-interval* and becomes equal to or greater than the **maximum** *retry-interval* configured, the subsequent retries are done at regular intervals of **maximum** *retry-interval* seconds until the call is established. Range is from 1 to 65535 seconds; the default is 60.
enable	Allows the soft connection to be set up. Enable is the default for the initial soft connection configuration. If the soft connection command is reentered for an existing connection, the default is the current enabled or disabled state.
disable	Prevents an initial soft connection from being set up, or tears down an existing connection.
redo-explicit	Applies only to existing soft connections and allows explicit paths to be respecified without tearing down connections. Existing connections are unaffected unless a reroute takes place, and then they will use the newer explicit path configuration.
explicit-path	The PNNI explicit path that is manually configured for routing a soft PVP, using the **atm pnni explicit-path** command.
precedence	The precedence number by which ATM PNNI explicit paths are assigned, from 1 to 3. You can assign up to three explicit paths to a soft PVP.
name *path-name*	The name of the ATM PNNI explicit path for routing soft PVPs.
identifier *path-id*	Specifies the path ID for the explicit path being configured to route soft PVPs.
upto *partial-entry-index*	Allows a subset of a longer explicit path to be used, so that all included nodes after the specified entry index will be disregarded. If the destination is reachable at any **next-node** or **segment-target**, the remaining included nodes in the explicit path are disregarded automatically. For more information, see the **atm pnni explicit-path next-node** and **atm pnni explicit-path segment-target** PNNI explicit path configuration commands.
only-explicit	If one or more explicit paths have been specified and if the explicit path fails, the soft connection remains down until it is retried at its next **retry-interval**. If this option is not specified, the system uses the standard on-demand routing instead of waiting for the next **retry interval**.
name *string*	A unique identifier, up to 16 characters, for the soft PVP connection. The name is unique per DSLAM for all connections. The name is nvgened to retain the binding across reloads.

Defaults See Syntax Description.

Command Modes Interface configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.2(5)DA	The **name** and **alternate-signalling tagging** keywords were added.

Usage Guidelines Obtain the destination port address before configuring a soft PVC by using the **show atm interface** or **show atm addresses** command on the destination DSLAM**.**

The creation of a soft PVC might be unsuccessful because of the following scenarios:

- A VPI or VCI collision at the source or destination DSLAM.
- The source or destination interface is not up (or autoconfiguration is not complete).
- The specified destination address is incorrect.

You can assign up to three explicit paths to a soft VC, by using precedence numbers 1 through 3. The system considers the precedence 1 explicit path as the primary path and tries it first. If it fails, the next precedence path is tried. You can specify explicit paths either by **name** or by **identifier**.

You can change the explicit path options without tearing down an existing soft PVC. Use the **redo-explicit** form of the command to respecify all of the explicit path options.

After configuring a soft PVC, use the **show atm vc interface** command on the source node (specify the source VPI and source VCI) to verify that the soft PVC is working and to see the explicit path that the software is using.

Note The configuration that displays for soft connections with explicit paths is always shown as two separate lines. The **redo-explicit** keyword is on the second line, even if it was originally configured through the use of a single command line.

Note To use the **atm soft-vc alternate-signalling tagging** command, you must shut down the interface and set the **upc** to **tag**.

Examples The following example shows how a user at the destination DSLAM displays the address of the destination port.

```
DSLAM> show atm address

Switch Address(es):
  47.0091.8100.0000.0005.312a.2c01.0005.312a.2c01.00 active
  NOTE: Switch addresses with selector bytes 01 through 7F
        are reserved for use by PNNI routing

PNNI Local Node Address(es):
  47.0091.8100.0000.0005.312a.2c01.0005.312a.2c01.01 Node 1

Soft VC Address(es):
  47.0091.8100.0000.0005.312a.2c01.4000.0c98.0010.00 ATM0/1
  47.0091.8100.0000.0005.312a.2c01.4000.0c98.0020.00 ATM0/2
```

```
47.0091.8100.0000.0005.312a.2c01.4000.0c98.0030.00 ATM0/3
47.0091.8100.0000.0005.312a.2c01.4000.0c98.0040.00 ATM0/4
47.0091.8100.0000.0005.312a.2c01.4000.0c98.0050.00 ATM0/5
47.0091.8100.0000.0005.312a.2c01.4000.0c98.0060.00 ATM0/6
47.0091.8100.0000.0005.312a.2c01.4000.0c98.0070.00 ATM0/7
47.0091.8100.0000.0005.312a.2c01.4000.0c98.0080.00 ATM0/8
47.0091.8100.0000.0005.312a.2c01.4000.0c98.0090.00 ATM0/9
47.0091.8100.0000.0005.312a.2c01.4000.0c90.00a0.00 ATM0/IMA0
47.0091.8100.0000.0005.312a.2c01.4000.0c90.00b0.00 ATM0/IMA1
47.0091.8100.0000.0005.312a.2c01.4000.0c90.00c0.00 ATM0/IMA2
47.0091.8100.0000.0005.312a.2c01.4000.0c90.00d0.00 ATM0/IMA3
```

The following example shows how to configure a soft-vc with the alternative tagging option set to forward.

```
DSLAM(config)# interface atm 0/1
DSLAM(config-if)# atm soft-vc alternate-signalling tagging fwd
```

Related Commands

Command	Description
atm pnni explicit-path	Creates or modifies PNNI explicit paths.
show atm addresses	Displays the active ATM addresses on a switch.
show atm vc	Displays all ATM virtual circuits (PVCs and SVCs) and traffic information.

auto-sync

To enter the auto-sync submode for automatically synchronizing the configuration/flash between the Cisco primary and secondary redundant NI-2s, use the **auto-sync** global configuration command.

auto-sync bootflash

auto-sync config

auto-sync exit

auto-sync flash

auto-sync running-config

Syntax Description

bootflash	Automatically synchronize the bootflash.
config	Automatically synchronizes the startup configuration and ifIndex-Table file.
exit	Exit the auto-sync configuration submode.
flash	Automatically synchronize the flash.
running-config	Automatically synchronize the running configuration file.

Defaults

- **auto-sync config**
- **auto-sync running-config**

Command Modes

Auto-sync configuration submode

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Usage Guidelines

The **auto-sync config** and **auto-sync running-config** global configuration commands are enabled by default. You need to use these commands only if you previously disabled the commands.

You must also manually synchronize the flash files and bootflash files before you can enable autosynchronization. Otherwise, when operation changes from the primary to the secondary device, the operation of the DSLAM might change if the software versions differ from one NI-2 to the other.

Examples

The following example enables autosynchronization of the bootflash files:

```
DSLAM# configure terminal
DSLAM(config)# auto-sync
DSLAM(config-auto-sync)# bootflash
```

The following example disables autosynchronization of the bootflash files:

```
DSLAM# configure terminal
DSLAM(config)# auto-sync
DSLAM(config-auto-sync)# bootflash
```

Related Commands

Command	Description
dir bootflash	Display the bootflash files for the primary NI-2 card.
dir flash	Display the flash files for the primary NI-2 card.
dir secondary-bootflash	Display the bootflash files for the secondary NI-2 card.
dir secondary-flash	Display the flash files for the secondary NI-2 card.
show running config	Display running configuration.

C and D Commands for Cisco DSLAMs with NI-2

This chapter documents commands that you use to configure Cisco DSLAMs with NI-2. Commands in this chapter are listed alphabetically. For information on how to configure DSL features, refer to the *Configuration Guide for Cisco DSLAMs with NI-2*.

Note Commands that are identical to those documented in the *Cisco IOS Configuration Fundamentals Command Reference* and the *ATM and Layer 3 Switch Router Command Reference* have been removed from this chapter.

This chapter discusses the following commands:

cap baud

cap bitrate

cap cpe-signature

cap interleaving-delay

cap margin

cap psdm

clear counters

clear ip dhcp binding

clear ip dhcp conflict

clear ip dhcp server statistics

clear ip route vrf

clear vpdn

client-identifier

client-name

clock source

cns config initial

cns config partial

cns event

debug cns config

debug cns event

debug ip dhcp server

default

default-router

dmt bitrate

dmt check-bytes

dmt codeword-size

dmt encoding trellis

dmt interleaving-delay

dmt margin

dmt minrate-blocking

dmt operating-mode

dmt overhead-framing

dmt power-management-additional-margin

dmt rate-adaptation enable

dmt rate-adaptation interval

dmt rate-adaptation margin

dmt training-mode

dns-server

domain-name

dsl atuc-1-4dmt rx-attenuation

dsl circuit

dsl-copy-profile

dsl-profile

dsl profile

dsl subscriber

dsl test atm self

cap baud

To enable upstream or downstream baud (symbol) rates, use the **cap baud** command in profile configuration mode. Use the **no** form of the command to disable a previously set baud rate.

cap baud {**downstream** *cap-baudrate* | **upstream** *cap-baudrate*}

no cap baud {**downstream** *cap-baudrate* | **upstream** *cap-baudrate*}

Syntax Description

downstream *cap-baudrate*	Enable a downstream baud rate. The valid value is 136 K.
upstream *cap-baudrate*	Enable an upstream baud rate. The valid values are 17 K and 68 K.

Defaults

Downstream: 136 Kbaud is enabled

Upstream: 68 Kbaud and 17 Kbaud are disabled

The following baud rates are always enabled and cannot be disabled:

Downstream: 340 Kbaud, 680 Kbaud, 952 Kbaud

Upstream: 136 Kbaud

Command Modes

Profile configuration

Command History

Release	Modification
12.0(8)DA	This command was introduced.

Usage Guidelines

Baud rates affect bit rates. Enabling more baud rates causes more bit rates to become available on the affected lines (see the "cap bitrate" section on page 3-5). However, the baud rates legally available to you might be determined by tariffs. Consult your organization's legal department before setting the baud rate.

The baud rate settings are mutually independent; you can enable or disable any baud rate without passing data because there are unconfigurable baud rates that you cannot disable (see the "Defaults" section).

Examples

The commands in this example disable the 136 Kbaud rate downstream and enable the 68 Kbaud rate upstream for the profile named issis:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile issis
DSLAM(cfg-dsl-profile)# no cap baud downstream 136k
DSLAM(cfg-dsl-profile)# cap baud upstream 68k
```

Related Commands

Command	Description
cap bitrate	Sets the downstream and upstream minimum or maximum bit rates.
dsl-profile	Creates a DSL profile or selects an existing profile for modification.
dsl profile	Attaches a profile to a specific port.
show dsl interface atm *slot#/port#*	Displays DSL and ATM status for a port.
show dsl profile [*profile name*]	Displays a specific profile or all profiles.

cap bitrate

To set the downstream and upstream minimum or maximum bit rates, use the profile configuration command **cap bitrate**. Use the **no** form of the command to set bit rates to default values.

cap bitrate minimum downstream *min-cap-bitrate* **upstream** *min-cap-bitrate*

cap bitrate maximum downstream *max-cap-bitrate* **upstream** *max-cap-bitrate*

no cap bitrate {**minimum** | **maximum**}

Syntax Description

min-cap-bitrate	If the line trains below this rate, the system generates an alarm. See the Usage Guidelines section for available values and for more information on alarms.
max-cap-bitrate	The rate at which the line attempts to train. If the line cannot train at the configured maximum rate, the modems attempt to train at the closest rate possible without exceeding the configured maximum. See the Usage Guidelines section for available values.

Defaults

Value Type	Default
Minimum downstream	0 kbps
Minimum upstream	0 kbps
Maximum downstream	640 kbps
Maximum upstream	91 kbps

Command Modes

Profile configuration

Command History

Release	Modification
12.0(8)DA	This command was introduced.

Usage Guidelines

Only the alarm subsystem uses the minimum bit rate settings. Cisco IOS asserts an alarm if the line card trains at a rate below the configured minimum bit rate. However, no alarm is generated when alarms are disabled for the profile. See the "alarms" section on page 2-11 for more information on enabling and disabling alarms.

Before you use the **cap bitrate** command, use the **cap baud** command to enable and disable baud rates. When you use the **cap bitrate** command, set the maximum bit rates, both downstream and upstream, before you set the minimum bit rates.

You must set baud and bit rate parameters in the order specified because the baud rates that you enable or disable affect the bit rates that are available to you. Also, the maximum bit rates you select affect the minimum bit rates that are available.

Table 3-1 shows bit rate values. In the Valid Values column, values that are always available are shown in bold. Values not shown in bold are unavailable under certain circumstances:

- Some upstream maximum bit rate values are available only when a particular downstream maximum bit rate is configured.
- Some downstream maximum values are available only when the 136 Kbaud downstream baud rate is enabled. (Use the **cap baud** command to disable and enable baud rates.)
- Some upstream maximum values are available only when the 68 Kbaud or 17 Kbaud upstream baud rates are enabled.

Table 3-1 CAP Bit Rate Values

Parameter	Direction	Valid Values (kbps)[1]	Default Value (kbps)
max-cap-bitrate	Downstream	256, 384, 512, **640**, 768, 896, **960**, 1024, **1280**, **1600**, **1920**, **2240**, **2560**, **2688**, **3200**, **4480**, **5120**, **6272**, **7168**	640
	Upstream	12, 34, 46, 51, 68, 85, 91, 102, 119, 136, 204, 272, 340, **408**, 476, 544, **680**, 816, **952**, **1088**	91
min-cap-bitrate	Downstream	Minimum: 0 Maximum: Equal to the currently configured downstream max-cap-bitrate	0
	Upstream	Minimum: 0 Maximum: Equal to the currently configured downstream max-cap-bitrate	0

1. Values printed in bold are always available.

Examples

The commands in this example set the maximum downstream and upstream bit rates to 7168 kbps and 1088 kbps respectively:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile issis
DSLAM(cfg-dsl-profile)# cap bitrate maximum downstream 7168 upstream 1088
```

Related Commands

Command	Description
alarms	Enables alarms in profile command mode.
cap baud	Enables upstream or downstream baud (symbol) rates.
dsl-profile	Creates a DSL profile or selects an existing profile for modification.
dsl profile	Attaches a profile to a specific port.
show dsl profile [*profile name*]	Displays a specific profile or all profiles.
show dsl interface atm *slot#/port#*	Displays DSL and ATM status for a port.

cap cpe-signature

The CPE signature indicates the supported feature set for CPE equipment. To set the CPE signature value for each configuration profile, use the **cap cpe-signature** command in profile configuration mode. Use the **no** form of the command to set the CPE signature to the default value.

cap cpe-signature *cpe-signature*

no cap cpe-signature

Syntax Description

cpe-signature	The range of CPE signature values is 0 to 127.

Defaults

The CPE signature is disabled (zero) by default.

Command Modes

Profile configuration

Command History

Release	Modification
12.0(8)DA	This command was introduced.

Usage Guidelines

If the CPE signature value that the CPE returns is less than the value configured on the DSLAM, the two devices do not train. When the CPE signature is set to its default value of 0 on the DSLAM, the feature is disabled; the DSLAM attempts to train with the CPE regardless of the signature value that the CPE returns.

Examples

In this example, the command sets the CPE signature to 103 for the DSL profile named issis:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile issis
DSLAM(cfg-dsl-profile)# cap cpe-signature 103
DSLAM(cfg-dsl-profile)# end
```

Related Commands

Command	Description
show dsl profile [*profile name*]	Displays a specific profile or all profiles.
show dsl interface atm *slot#/port#*	Displays DSL and ATM status for a port.

cap interleaving-delay

To set the interleaving delay for a profile, use the **cap interleaving-delay** command in profile configuration mode. Use the **no** form of the command to set interleaving delay to the default value.

cap interleaving-delay {**short | long | none**}

no cap interleaving-delay {**short | long | none**}

Syntax Description

short	Configures a small amount of delay and turns on Reed-Solomon error correction. See the Usage Guidelines below for details.
long	Configures a larger amount of delay and turns on Reed-Solomon error correction. See the Usage Guidelines below for details.
none	Configures no delay and turns off Reed-Solomon error correction. This value is valid only when the downstream baud 136 K is enabled, and for bit-rate settings that use 136 K. See the Usage Guidelines below for details. **Note** If you set interleaving delay to **none**, the subscriber line might provide service at a higher bit rate than the one configured. Setting interleaving delay to **none** turns off Reed-Solomon error correction, and turning off error correction reduces the overhead on the line, which leaves more bandwidth available to the subscriber.

Defaults

long

Command Modes

Profile configuration

Command History

Release	Modification
12.0(8)DA	This command was introduced.

Usage Guidelines

This command changes the amount of delay by setting interleaving depth. It affects downstream traffic only.

Table 3-2 shows the amount of delay (in milliseconds) that results from various combinations of baud rate, constellation, and interleaving delay settings (short or long), in the downstream direction. Interleaving is not used on upstream traffic.

Table 3-2 Downstream Interleaving Delay

Constellation	Short or Long Delay	136 Kbaud	340 Kbaud	680 Kbaud	952 Kbaud
8	short	4.4 ms	4.4 ms	—	—
	long	49 ms	49 ms	—	—

Table 3-2 Downstream Interleaving Delay (continued)

Constellation	Short or Long Delay	136 Kbaud	340 Kbaud	680 Kbaud	952 Kbaud
16	short	3.0 ms	3.0 ms	3.0 ms	2.7 ms
	long	31 ms	31 ms	16 ms	11 ms
32	short	2.3 ms	2.3 ms	—	—
	long	24 ms	24 ms	—	—
64	short	1.9 ms	1.9 ms	1.8 ms	1.7 ms
	long	19 ms	19 ms	9.6 ms	6.8 ms
128	short	1.6 ms	1.6 ms	—	—
	long	16 ms	16 ms	—	—
256	short	1.4 ms	1.4 ms	1.4 ms	1.2 ms
	long	14 ms	14 ms	6.8 ms	5.0 ms
256 uncorrected	short	1.3 ms	1.3 ms	1.2 ms	1.0 ms
	long	12 ms	12 ms	6.0 ms	4.3 ms

You can choose the interleaving-delay option **none** only when you enable the 136 K downstream baud rate.

If you configure the interleaving-delay to **none** but the line card trains at a downstream bit rate that uses a baud rate that is other than 136 K, the actual interleaving-delay value that the system uses is **short**.

The left column of Table 3-3 lists the downstream maximum bit rates for which the interleaving delay setting **none** is valid. Because the **none** setting turns off Reed-Solomon error correction, the actual bit rate on the line will be higher than the configured bit rate, as shown in the right column. The actual bit rate exceeds the configured bit rate because turning off Reed-Solomon error correction reduces the overhead on the line, leaving more bandwidth available to the subscriber.

Table 3-3 Configured and Actual Bit Rates with Interleaving Delay Set to none

Configured Downstream Maximum Bit Rate	Actual Downstream Maximum Bit Rate
256 kbps	272 kbps
384 kbps	408 kbps
512 kbps	544 kbps
640 kbps	680 kbps
768 kbps	816 kbps
896 kbps	952 kbps
1024 kbps	1088 kbps

Examples

In this example, the command sets the interleaving-delay value to **none**:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile issis
DSLAM(cfg-dsl-profile)# cap interleaving-delay none
DSLAM(cfg-dsl-profile)# end
```

Related Commands

Command	Description
show dsl interface atm *slot#/port#*	Displays DSL and ATM status for a port.
show dsl profile [*profile name*]	Displays a specific profile or all profiles.

cap margin

To set the upstream and downstream signal-to-noise ratio (SNR) margin values for a CAP profile, use the **cap margin** command. Use the **no** form of the command to set the margins to the default values.

cap margin downstream *cap-margin* **upstream** *cap-margin*

no cap margin downstream *cap-margin* **upstream** *cap-margin*

Syntax Description

cap-margin	Upstream and downstream SNR margins in decibels. The range of values is 0 to 12.

Defaults

Downstream: 3 dB
Upstream: 6 dB

Command Modes

Profile configuration

Command History

Release	Modification
12.0(8)DA	This command was introduced.

Usage Guidelines

SNR margin values are in decibels.

Examples

In this example, the command sets the SNR margin at 8 dB downstream and 5 dB upstream for the DSL profile issis:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile issis
DSLAM(cfg-dsl-profile)# cap margin downstream 8 upstream 5
DSLAM(cfg-dsl-profile)# end
```

Related Commands

Command	Description
show dsl interface atm *slot#/port#*	Displays DSL and ATM status for a port.
show dsl profile [*profile name*]	Displays a specific profile or all profiles.

cap psdm

To set the CAP power spectral density mask (PSDM) upstream and downstream values, use the **cap psdm** command in profile configuration mode. Use the **no** form of the command to set PSDM to default values.

cap psdm downstream *psdm-value* **upstream** *psdm-value*

no cap psdm downstream *psdm-value* **upstream** *psdm-value*

Syntax Description

psdm-value	Downstream values: –37, –40, –43, –46, –49, –52 Upstream values: –38, –41, –44, –47, –50, –53

Defaults

Downstream: –40 dB m/Hz
Upstream: –38 dB m/Hz

Command Modes

Profile configuration

Command History

Release	Modification
12.0(8)DA	This command was introduced.
12.1(1)DA	The downstream default was changed from –37 dB to –40 dB.

Usage Guidelines

PSDM values are in decibels relative to one milliwatt.

Examples

In this example, the command sets the CAP PSDM value to –37 dB downstream and –41 dB upstream:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile issis
DSLAM(cfg-dsl-profile)# cap psdm downstream -37 upstream -41
DSLAM(cfg-dsl-profile)# end
```

Related Commands

Command	Description
show dsl interface atm *slot#/port#*	Displays DSL and ATM status for a port.
show dsl profile [*profile name*]	Displays a specific profile or all profiles.

clear counters

To clear the interface counters, use the **clear counters** privileged EXEC command.

clear counters [*type slot/port*]

Syntax Description

type	Specifies the interface type; one of the keywords listed in Table 3-4.
slot	Number of the slot being configured. Refer to the appropriate hardware manual for slot and port information.
port	Number of the port being configured. Refer to the appropriate hardware manual for slot and port information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

This command clears all the current interface counters from the interface unless you specify the optional arguments *type* and *number* to clear only a specific interface type (serial, Ethernet, Token Ring, and so on). Table 3-4 lists the command keywords and their descriptions.

Note This command does not clear counters that were retrieved using SNMP, but only those seen with the **show interface** EXEC command.

Table 3-4 clear counters Interface Type Keywords

Keyword	Interface Type
ATM	ATM interface
async	Asynchronous interface
bvi	Bridge-Group Virtual Interface
ethernet	IEEE 802.3
Group-Async	Async Group Interface
Lex	Lex interface
Line	Terminal line
loopback	Loopback interface
multilink	Multilink-group interface
null	Null interface
tunnel	Tunnel interface
Vif	PGM Multicast Host interface

Table 3-4 clear counters Interface Type Keywords (continued)

Keyword	Interface Type
Virtual-Template	Virtual Template interface
Virtual-TokenRing	Virtual TokenRing

Examples

The following example clears all interface counters:

```
DSLAM# clear counters
```

The following example clears the atm 0/1 interface counters:

```
DSLAM# clear counters atm 0/1
```

Related Commands

Command	Description
show interfaces	Displays the statistical information that is specific to an interface.

clear ip dhcp binding

To delete an automatic address binding from the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server database, use the **clear ip dhcp binding** privileged EXEC command.

clear ip dhcp binding *address* | ***

Syntax Description

address	The address of the binding you want to clear.
*	Clears all automatic bindings.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

Typically, the address denotes the client IP address. When you use the asterisk (*) character as the address parameter, DHCP clears all automatic bindings.

Use the **no ip dhcp pool** global configuration command to delete a manual binding.

Examples

The following example deletes the address binding 10.12.1.99 from a DHCP server database:

```
DSLAM# clear ip dhcp binding 10.12.1.99
```

Related Commands

Command	Description
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.

clear ip dhcp conflict

To clear an address conflict from the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server database, use the **clear ip dhcp conflict** privileged EXEC command.

clear ip dhcp conflict *address* | ***

Syntax Description

address	The IP address of the host that contains the conflicting address you want to clear.
*	Clears all address conflicts.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The server detects conflicts using a ping session. The client detects conflicts using gratuitous Address Resolution Protocol (ARP). If you use the asterisk (*) character as the address parameter, DHCP clears all conflicts.

Examples

The following example shows an address conflict of 10.12.1.99 being deleted from the DHCP server database:

```
DSLAM# clear ip dhcp conflict 10.12.1.99
```

Related Commands

Command	Description
show ip dhcp conflict	Displays address conflicts found by a Cisco IOS DHCP server when addresses are offered to the client.

clear ip dhcp server statistics

To reset all Cisco IOS Dynamic Host Configuration Protocol (DHCP) server counters, use the **clear ip dhcp server statistics** privileged EXEC command.

clear ip dhcp server statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The **show ip dhcp server statistics** command displays DHCP counters. All counters are cumulative. The counters are initialized, or set to zero, with this command.

Examples

The following example resets all DHCP counters to zero:

```
DSLAM# clear ip dhcp server statistics
```

Related Commands

Command	Description
show ip dhcp server statistics	Displays Cisco IOS DHCP server statistics.

clear ip route vrf

To remove routes from the VRF routing table, use the **clear ip route vrf** EXEC command.

clear ip route vrf *vrf-name* {***** | **network** [**mask**]}

Syntax Description

vrf-name	Name of the VPN routing or forwarding instance (VRF) for the static route.
*****	Delete all routes for a VRF.
network	Specify destination routes to be removed.
mask	(Optional) Mask for the specified network destination, in dotted-decimal format.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

Use this command to clear routes from the routing table. Use the asterisk (*) to delete all routes from the forwarding table for a specified VRF, or enter the address and mask of a particular network to delete the route to that network.

Examples

The following example shows how to remove the route to the network 10.13.0.0 in the vpn1 routing table:

```
DSLAM# clear ip route vrf vpn1 10.13.0.0
```

Related Commands

Command	Description
show ip route vrf	Displays the IP routing table associated with a VRF.

clear vpdn

To shut down a specified tunnel and all sessions within the tunnel, use the **clear vpdn tunnel** EXEC command.

clear vpdn tunnel {**l2f** *nas-name* | **l2tp** [*remote name*] | **pppoe** | **pptp**}

Syntax Description

l2f	Specifies the l2f tunnel protocol.
nas-name	Name of the network access server at the far end of the tunnel.
l2tp	Specifies the l2tp tunnel protocol.
remote name	(Optional) Host name of the tunnel peer. At the LNS, this is the name of the L2TP access concentrator (LAC); at the LAC, this is the name of the L2TP network server (LNS).
pppoe	Specifies the PPPoE tunnel protocol.
pptp	Specifies the PPTP tunnel protocol.

Note The **l2f** and **pptp** keywords are not supported by Release 12.2(1b).

Command Modes

EXEC

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

Use this command to clear a specific tunnel and all sessions within the tunnel.

Use this command to isolate problems by forcing a tunnel to come down without unconfiguring the tunnel (the tunnel can be restarted immediately by a user logging in).

If you are using the **l2tp** keyword, you can clear the tunnel by matching either the remote name or remote name and local name.

Examples

The following example clears a tunnel to a remote peer named sophia:

```
DSLAM> clear vpdn tunnel l2tp mugsy sophia
```

client-identifier

To specify a unique identifier (in dotted-hexadecimal notation) for a Microsoft Dynamic Host Configuration Protocol (DHCP) client, use the **client-identifier** DHCP pool configuration command. It is valid for manual bindings only. Use the **no** form of this command to delete the client identifier.

client-identifier *unique-identifier*

no client-identifier

Syntax Description

unique-identifier	The distinct identification of the client in dotted-hexadecimal notation, for example, 01b7.0813.8811.66.

Defaults

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

Microsoft DHCP clients require client identifiers instead of hardware addresses. The client identifier is formed by concatenating the media type and the MAC address. For example, the Microsoft client identifier for Ethernet address b708.1388.f166 is 01b7.0813.88f1.66, where 01 represents the Ethernet media type. For a list of media type codes, refer to the "Address Resolution Protocol Parameters" section of RFC 1700, *Assigned Numbers*.

Examples

The following example specifies the client identifier for Mac address b7.0813.8811.66 in dotted-hexadecimal notation:

```
DSLAM(config)# ip dhcp pool 1
DSLAM(dhcp-config)# client-identifier 01b7.0813.8811.66
```

Related Commands

Command	Description
hardware-address	Specifies the hardware address of a DHCP client.
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

client-name

To specify the name of a Dynamic Host Configuration Protocol (DHCP) client, use the **client-name** DHCP pool configuration command. The client name should not include the domain name. Use the **no** form of this command to remove the client name.

client-name *name*

no client-name

Syntax Description

name	Specifies the client name, using standard ASCII characters. The client name should not include the domain name. For example, the name **mars** should not be specified as **mars.cisco.com**.

Defaults

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Examples

The following example specifies a string *client1* to be the name of the client:

```
DSLAM(config)# ip dhcp pool 1
DSLAM(dhcp-config)# client-name client1
```

Related Commands

Command	Description
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

clock source

To select a transmit clock source for an atm interface, use the **clock source** interface configuration command. When you assign a link to an IMA group interface, this command has no effect unless the link is the common clock source in the CTC IMA group. When you change the link back from an IMA group interface to g.804 mode, the system reflects the changes. To return the clock source to the default, use the **no** form of this command.

clock source {loop-timed | network-derived} [protection | working | <cr>]

Syntax Description

loop-timed	The transmit clock is derived from the local oscillator on the atm interface.
network-derived	The transmit clock is derived from the network clock that you specify at highest priority when you use the **network-clock-select** global configuration command.
protection	The fiber that is local to the NI-2 card in slot 11.
working	The fiber that is local to the NI-2 card in slot 10.
<cr>	Both protection and working fibers.

Defaults

The clock source is network derived by default (**clock source network-derived**).

Command Modes

Interface configuration.

Command History

Release	Modification
12.1(4)DA	This command was introduced.
12.1(7)DA	The keywords **working** and **protection** were added.

Usage Guidelines

The protection and working keywords apply only to SONET automatic protection switching.

Examples

The following example shows how to enable the loop-timed clocking mode on the protection fiber on atm 0/2:

```
DSLAM> enable
DSLAM# configure terminal
DSLAM(config)# interface atm 0/2
DSLAM(config-if)# clock source loop-timed protection
```

Related Commands

Command	Description
show controllers	Displays information on working and protection fibers.
show network-clocks	Displays the local clock and the peer clock source.

cns config initial

To start the Cisco Network Services (CNS) Configuration Agent and initiate an initial configuration, use the **cns config initial** command in global configuration mode. To remove the existing **cns config initial** command from the running configuration of the routing device, use the **no** version of this command.

cns config initial *host*

no cns config initial *host*

Syntax Description

host	Host name or IP address of the configuration server.

Defaults

Default port number is 80. Default web page of the initial configuration is /Config/config.asp.

Command Modes

Global configuration

Command History

Release	Modification
12.2(5)DA	This command was introduced.

Usage Guidelines

Use this command to start the CNS Configuration Agent and begin an initial configuration. The Configuration Agent gets the initial configuration for the routing device from the specified server. When this command is used with the **cns event** command, the event bus displays one of the following status messages:

- cisco.cns.config.failure—CNS Configuration Agent detected a syntax error or unsupported hardware.
- cisco.cns.config.success—CNS Configuration Agent successfully applied the initial configuration.
- cisco.cns.config.warning—CNS Configuration Agent fully applied the initial configuration, but encountered possible semantic errors.

Related Commands

Command	Description
debug cns config	Turns on debug messages related to the CNS Configuration Agent.
show cns config	Displays information about the CNS Configuration Agent.

cns config partial

To start the CNS Configuration Agent and initiate a partial configuration, use the **cns config partial** command in global configuration mode. To shut down the partial configuration, use the **no** version of this command.

cns config partial *host*

no cns config partial *host*

Syntax Description

host	Host name or IP address of the configuration server.

Defaults

Default port number is 80.

Command Modes

Global configuration

Command History

Release	Modification
12.2(5)DA	This command was introduced.

Usage Guidelines

Use this command to start the CNS Configuration Agent and initiate a partial configuration. One of the following status messages displays:

- cisco.cns.config.failure—CNS Configuration Agent detected a syntax error or unsupported hardware.
- cisco.cns.config.success—CNS Configuration Agent successfully applied the partial configuration.
- cisco.cns.config.warning—CNS Configuration Agent fully applied the partial configuration, but encountered possible semantic errors.

Related Commands

Command	Description
debug cns config	Turns on debug messages related to the CNS Configuration Agent.
show cns config	Displays information about the CNS Configuration Agent.

cns event

To configure the Cisco Networking Services (CNS) event gateway, use the **cns event** command in global configuration mode. To remove the specified event gateway from the gateway list, use the **no** version of this command

cns event *host*

no cns event *host*

Syntax Description

host	Host name or IP address of the event gateway.

Defaults

Default port number is 11011.

Command Modes

Global configuration

Command History

Release	Modification
12.2(5)DA	This command was introduced.

Usage Guidelines

Use this command to enable the CNS Event Gateway.

Related Commands

Command	Description
debug cns config	Turns on debug messages related to the CNS Configuration Agent.
show cns event	Displays information about the CNS Event Agent.

debug cns config

To turn on debug messages related to the CNS Configuration Agent, use the **debug cns config** command in EXEC mode. To turn off debug messages related to the Configuration Agent, use the **no** version of this command.

debug cns config {**all | connection | agent**}

no debug cns config {**all | connection | agent**}

Syntax Description

all	Displays all debug messages.
connection	Displays connection handler messages.
agent	Displays Configuration Agent messages.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2(5)DA	This command was introduced.

Usage Guidelines

Use this command to turn on or off debug messages related to the Configuration Agent.

Related Commands

Command	Description
cns config initial	Starts the initial CNS Configuration Agent.
cns config partial	Starts the partial CNS Configuration Agent.
show cns config	Displays information about the CNS Configuration Agent.

debug cns event

To turn on debug messages related to the Cisco Networking Services (CNS) event gateway, use the **debug cns event** command in EXEC mode. To turn off the debug messages related to the event gateway, use the **no** version of this command.

debug cns event {**all | subscriber | agent | connection**}

no debug cns event {**all | subscriber | agent | connection**}

Syntax Description

all	Logs all debug messages about the event gateway.
subscriber	Logs messages about the event subscriber.
agent	Logs messages about the event agent.
connection	Logs messages about connections to the gateway.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2(5)DA	This command was introduced.

Usage Guidelines

Use this command to turn on or off debug messages related to the event gateway.

Related Commands

Command	Description
cns event	Configures the CNS event gateway.
show cns event	Displays information about the CNS event agent.

debug ip dhcp server

To enable Cisco IOS Dynamic Host Configuration Protocol (DHCP) server debugging, use the **debug ip dhcp server** privileged EXEC command. Use the **no** form of this command to disable DHCP server debugging.

debug ip dhcp server {**events | packets | linkage**}

no debug ip dhcp server {**events | packets | linkage**}

Syntax Description

events	Reports server events, such as address assignments and database updates.
packets	Decodes DHCP receptions and transmissions.
linkage	Displays database linkage information (such as parent-child relationships in a radix tree).

Defaults

DHCP server debugging is not enabled.

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Examples

The first example below shows a combination of DHCP server events and decoded receptions and transmissions. The second example below shows database linkage information.

```
DSLAM# debug ip dhcp server events
DSLAM# debug ip dhcp server packets
DHCPD:DHCPDISCOVER received from client 0b07.1134.a029 through relay 10.1.0.253.
DHCPD:assigned IP address 10.1.0.3 to client 0b07.1134.a029.
DHCPD:Sending DHCPOFFER to client 0b07.1134.a029 (10.1.0.3).
DHCPD:unicasting BOOTREPLY for client 0b07.1134.a029 to relay 10.1.0.253.
DHCPD:DHCPREQUEST received from client 0b07.1134.a029.
DHCPD:Sending DHCPACK to client 0b07.1134.a029 (10.1.0.3).
DHCPD:unicasting BOOTREPLY for client 0b07.1134.a029 to relay 10.1.0.253.
DHCPD:checking for expired leases.

DSLAM# debug ip dhcp server linkage
DHCPD:child  pool:10.1.0.0 / 255.255.0.0 (subnet10.1)
DHCPD:parent pool:10.0.0.0 / 255.0.0.0 (net10)
DHCPD:child  pool:10.0.0.0 / 255.0.0.0 (net10)
DHCPD:pool (net10) has no parent.
DHCPD:child  pool:10.1.0.0 / 255.255.0.0 (subnet10.1)
DHCPD:parent pool:10.0.0.0 / 255.0.0.0 (net10)
DHCPD:child  pool:10.0.0.0 / 255.0.0.0 (net10)
DHCPD:pool (net10) has no parent.
```

Related Commandss

Command	Description
show ip dhcp bindings	Displays address bindings on the Cisco IOS DHCP server.
show ip dhcp database	Displays Cisco IOS DHCP server database agent information.

default

To reset a VPDN group command or a VPDN subgroup command to its default value, use the **default** command.

default {**accept-dialin** | **accept-dialout** | **ip** | **request-dialin** | **request-dialout** | **source-ip**}

Syntax Description

accept-dialin	Removes the accept-dialin group from the VPDN group.
accept-dialout	Removes the accept-dialout group from the VPDN group.
description	Description for this VPDN group • request-dialin—VPDN request-dialin group configuration • request-dialout—VPDN request-dialout group configuration • source-ip—Set source IP address for this vpdn-group
ip	IP settings for the tunnel.
request-dialin	Removes the request-dialin group from the VPDN group.
request-dialout	Removes the request-dialout group from the VPDN group.
source-ip	Removes the **source-ip** command from the VPDN group.

Defaults

Disabled

Command Modes

VPDN group mode

VPDN subgroup modes

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

Caution Using the **default** command is similar to using the **no** form of a command.

Examples

The following example shows an LNS configured to accept L2F dial-in and L2TP dial-out:

```
DSLAM(config)# vpdn enable
DSLAM(config)# vpdn-group 1
DSLAM(config-vpdn)# accept-dialin
DSLAM(config-vpdn-acc-in)# protocol l2tp
DSLAM(config-vpdn-acc-in)# virtual-template 1
DSLAM(config-vpdn-acc-in)# local name reuben
DSLAM(config-vpdn-acc-in)# initiate-to ip 10.3.2.1
DSLAM(config-vpdn-acc-in)# l2f ignore-mid-sequence
DSLAM(config-vpdn-acc-in)# l2tp ip udp checksum
```

If you then issue the **default protocol** command in request-dialout mode, the configuration will look like this:

```
DSLAM(config)# vpdn-group 1
DSLAM(config-vpdn)# accept-dialin
DSLAM(config-vpdn-acc-in)# protocol l2f
DSLAM(config-vpdn-acc-in)# virtual-template 1
DSLAM(config-vpdn-req-out)# local name reuben
DSLAM(config-vpdn-req-out)# initiate-to ip 10.3.2.1
DSLAM(config-vpdn-req-out)# l2f ignore-mid-sequence
```

If you issue the **no accept-dialin** command when the LNS is configured as in the first example, the configuration will change to this:

```
DSLAM(config)# vpdn-group 1
DSLAM(config-vpdn)# request-dialout
DSLAM(config-vpdn-req-out)# protocol l2tp
DSLAM(config-vpdn-req-out)# pool-member 1
DSLAM(config-vpdn-req-out)# local name reuben
DSLAM(config-vpdn-req-out)# initiate-to ip 10.3.2.1
DSLAM(config-vpdn-req-out)# l2tp ip udp checksum
```

default-router

To specify the default router list for a Dynamic Host Configuration Protocol (DHCP) client, use the **default-router** DHCP pool configuration command. Use the **no** form of this command to remove the default router list.

default-router *address* [*address2 ... address8*]

no default-router

Syntax Description

address	Specifies the IP address of a router. One IP address is required, although you can specify up to eight addresses in one command line.

Defaults

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet. You can specify up to eight routers in the list. Routers are listed in order of preference (address1 for the most preferred router, address2 for the next most preferred router, and so on).

Examples

The following example specifies 10.12.1.99 as the IP address of the default router:

```
DSLAM(config)# ip dhcp pool 1
DSLAM(dhcp-config)# default-router 10.12.1.99
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

dmt bitrate

To set the maximum and minimum allowed bit rates for the fast or interleaved DMT profile parameters, use the **dmt bitrate** profile configuration command. To reset this command to the default value, use the **no** form of this command.

dmt bitrate maximum {fast | interleaved} downstream *dmt-bitrate* **upstream** *dmt-bitrate*

dmt bitrate minimum {fast | interleaved} downstream *dmt-bitrate* **upstream** *dmt-bitrate*

Syntax Description

dmt-bitrate	The DMT bit rate is given as a multiple of 32 kbps. If you enter a nonmultiple of 32 kbps, the system rejects and ends the command. See the allowed ranges and default values in Table 3-5 on page 3-33.
fast	DMT fast latency path.
interleaved	DMT interleaved latency path.

Defaults

- The default **no dmt bitrate maximum interleaved** sets the maximum downstream and upstream interleaved bit rate to 640 and 128 kbps respectively. This command causes the port to retrain.
- The default **no dmt bitrate maximum fast** sets both the maximum downstream and upstream fastpath bit rates to zero. This command causes the port to attempt to retrain. We do not recommend this command because the line will not train.
- The default **no dmt bitrate minimum interleaved** sets both the minimum downstream and upstream interleaved bit rates to zero. This command does not cause the port to retrain.
- The default **no dmt bitrate minimum fast** sets both the minimum downstream and upstream fastpath bit rates to zero. This command does not cause the port to retrain.

Command Modes

Profile configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.1(5)DA	The **fast** keyword was added.

Usage Guidelines

Only the alarm subsystem uses the minimum bit rate settings. Cisco IOS asserts an alarm if the line card trains at a rate below the configured minimum bit rate. However, no alarm is generated when alarms are disabled. See the "alarms" section on page 2-11 for more information on enabling and disabling alarms.

If alarms are enabled for the profile, setting the DMT minimum bit rate to 0 disables the associated DMT minimum bit rate alarm.

Table 3-5 lists the allowable DMT bit rate ranges and default values.

Table 3-5 Allowable Ranges and Default Values for DMT Bit Rates

		Downstream			Upstream		
Configuration Parameter	**Data Path**	**Aggregate Range (kbps)**	**Path Range (kbps)**	**Path Default (kbps)**	**Aggregate Range (kbps)**	**Path Range (kbps)**	**Path Default (kbps)**
DMT bit rate max	Fast	8064 to 32	8064 to 32	0	864 to 32	864 to 0	0
DMT bit rate min	Fast	8064 to 32	8064 to 0	0	864 to 32	864 to 0	0
DMT bit rate max	Interleaved	8064 to 32	8064 to 32	640	864 to 32	864 to 0	128
DMT bit rate min	Interleaved	8064 to 32	8064 to 0	0	864 to 0	864 to 0	0

Caution This command causes the port to retrain when you change the value of the bit rate parameter.

Setting a parameter to its current value does not cause a retrain. If a port is training when you change the parameter, the port untrains and retrains to the new parameter.

Examples

In this example, the command sets the maximum interleaved bit rate of the default profile to 3200 kbps downstream and 640 kbps upstream:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile default
DSLAM(cfg-dsl-profile)# dmt bitrate maximum interleaved downstream 3200 upstream 640
```

Related Commands

Command	Description
show dsl profile [*profile name*]	Displays a specific profile or all profiles.

dmt check-bytes

To set upstream and downstream forward error correction (FEC) check (redundancy) bytes, use the **dmt-checkbytes** profile configuration command. To reset this command to the default value, use the **no** form of this command.

dmt check-bytes {fast | interleaved} downstream *bytes* **upstream** *bytes*

Syntax Description

bytes	Upstream and downstream FEC check bytes. The allowed values are 0, 2, 4, 6, 8, 10, 12, 14, and 16.
fast	DMT fast latency path.
interleaved	DMT interleaved latency path.

Defaults

Latency Path	Downstream	Upstream
fast	0	0
interleaved	16	16

Command Modes

Profile configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.1(6)DA	The **fast** keyword was added.

Usage Guidelines

Caution This command causes the port to retrain when you change the *check-bytes* parameter.

Increasing the number of check bytes improves error correction but slows performance. Set FEC check bytes for a specific profile.

Setting a parameter to its current value does not cause a retrain. If a port is training when you change the parameter, the port untrains and retrains to the new parameter.

Conditions on the line, the configured bit rate, and the capabilities of the ATU-R CPE affect the achievable value for this parameter. As a result, the check-bytes value to which the line trains might be smaller than the value you configure. If you want to use more check bytes than the system is allowing you, use the **dmt bitrate** command to reduce the bit rate.

Use the command **show dsl interface atm** *slot#/port#* to display the configured and actual check-byte values for the connection.

Examples In this example, the command sets the interleaved FEC check-bytes for the default profile to 12 downstream and 6 upstream:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile default
DSLAM(cfg-dsl-profile)# dmt check-bytes interleaved downstream 12 upstream 6
```

Related Commands None.

dmt codeword-size

To set codeword size for upstream and downstream FEC check (redundancy) bytes, use the **dmt codeword-size** command.

dmt codeword-size downstream {*symbols* | **auto**} **upstream** {*symbols* | **auto**}

Syntax Description

symbols	The allowable values for codeword size (in symbols for each Reed-Solomon codeword) are 1, 2, 4, 8, and 16.
auto	If you select a codeword size of **auto**, the system calculates the number of symbols for each codeword according to the achievable DMT bit rate.

Defaults

Downstream: auto

Upstream: auto

Command Modes

Profile configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

Caution This command causes the port to retrain when you change the parameter.

Setting a parameter to its current value does not cause a retrain. If a port is training when you change this parameter, the port untrains and retrains to the new parameter.

Note Conditions on the line and the capabilities of the ATU-R CPE affect the achievable value for this parameter. As a result, the codeword-size value to which the line trains might not be the same as the value you configure.

Examples

In this example, the command sets the codeword size for the default profile to 8 upstream and to auto downstream:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile default
DSLAM(cfg-dsl-profile)# dmt codeword-size downstream auto upstream 8
```

Related Commands

None

dmt encoding trellis

Trellis coding is a method of performing forward error correction. Improved error correction involves a decrease in speed. You enable or disable trellis coding for a specific profile.

To enable trellis coding for a profile, use the **dmt encoding trellis** command. To disable trellis coding for a profile, use the **no** form of the command.

dmt encoding trellis

no dmt encoding trellis

Syntax Description

This command has no keywords or arguments.

Defaults

Disabled

Command Modes

Profile configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

Caution This command causes the port to retrain when you change the parameter.

Setting a parameter to its current value does not cause a retrain. If a port is training when you change this parameter, the port untrains and retrains to the new parameter.

Examples

In this example, the command turns off dmt encoding trellis for the default profile:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile default
DSLAM(cfg-dsl-profile)# no dmt encoding trellis
```

Related Commands

None.

dmt interleaving-delay

To set the interleaving delay parameter, use the **dmt interleaving-delay** command.

dmt interleaving-delay downstream *delay-in-usecs* **upstream** *delay-in-usecs*

Syntax Description

delay-in-usecs	Enter the interleaving delay in microseconds. Allowable values are 0, 1000, 2000, 4000, 8000, and 16000 microseconds.

Defaults

Downstream: 16000 microseconds

Upstream: 16000 microseconds

Command Modes

Profile configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

Caution This command causes the port to retrain when you change the parameter.

Setting this parameter to its current value does not cause a retrain. If a port is training when you change the value, the port untrains and retrains to the new value.

Note Conditions on the line and the capabilities of the ATU-R CPE affect the achievable value for this parameter. As a result, the interleaving-delay value to which the line trains might not be the same as the value you configure.

Examples

In this example, the command sets the interleaving delay of the default profile to 2000 microseconds downstream and 4000 microseconds upstream:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile default
DSLAM(cfg-dsl-profile)# dmt interleaving-delay downstream 2000 upstream 4000
```

Related Commands

None

dmt margin

To set upstream and downstream signal-to-noise ratio (SNR) margins for a DMT profile, use the **dmt margin** command. To reset this command to the default value, use the **no** form of this command.

dmt margin downstream *dmt-margin* **upstream** *dmt-margin*

Syntax Description

dmt-margin	Enter the upstream and downstream SNR margins in decibels. The range is 0 to 15.

Defaults

Downstream: 6 dB

Upstream: 6 dB

Command Modes

Profile configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

Caution This command causes the port to retrain when you change the parameter.

Setting a parameter to its current value does not cause a retrain. If a port is training when you change this value, the port untrains and retrains to the new value.

Note Conditions on the line and the capabilities of the ATU-R CPE affect the achievable value for this parameter. As a result, the DMT margin value to which the line trains might be higher than the value you configure.

Examples

In this example, the command sets the SNR DMT margins of the default profile to 12 dB downstream and 6 dB upstream:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile default
DSLAM(cfg-dsl-profile)# dmt margin downstream 12 upstream 6
```

Related Commands

None.

dmt minrate-blocking

To force a port *not* to retrain when actual bit rates fall below the values configured in the **dmt bitrate minimum** command, use the **dmt minrate-blocking** command. To disable dmt minrate-blocking, use the **no** form of the command.

dmt minrate-blocking

Syntax Description

This command has no arguments or keywords.

Defaults

The default configuration, **no dmt minrate-blocking**, generates a minor alarm when the bit rates on a DMT port violate the minimum allowed bit rates that are specified in the **dmt bitrate minimum** command (if alarms are enabled in the DSL profile).

Command Modes

Profile configuration

Command History

Release	Modification
12.1(6)DA	This command was introduced.

Usage Guidelines

To specify the bit rate below which a DMT port will not retrain, use the **dmt bitrate minimum** command.

Examples

The following example describes how to enable **dmt minrate-blocking**:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile 8xDMT
DSLAM(cfg-dsl-profile)# dmt minrate-blocking
```

dmt operating-mode

To modify the operating mode of a line in the DSL profile, use the **dmt operating-mode** command. To set the operating mode to the default value, use the **no** form of the command.

dmt operating-mode {**auto** | **g992-1** | **g992-2** | **t1-413**}

no dmt operating-mode

Syntax Description

auto	In this mode, the ATU-C automatically detects the capabilities of the ATU-R CPE and uses a startup sequence specified by G.992.1, G.992.2, or T1.413-1998. The default for an ADSL line is auto mode.
g992-1	In this mode, the ATU-C requests the G994.1 startup sequence. After startup, the line complies to G992.1 operation.
g992-2	In this mode, the ATU-C requests the G994.1 startup sequence. After startup, the line complies to G992.2 operation. (G992.2 is also known as G.lite.)
t1-413	In this mode, the ATU-C requests the T1.413-1998 startup sequence. After startup, the line complies to T1.41-1998 operation.

Defaults

auto

Command Modes

Profile configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.1(1)DA	The **g992-1**, **g992-2** , and **t1-413** keywords were added; the **splitterless** keyword was removed.

Usage Guidelines

Caution This command causes the port to retrain when you change the parameter.

If a port is training when you change the current value, the port untrains and retrains to the new value.

Note Not every CPE type is compatible with all operating modes. If you misconfigure the operating mode, the port might not train.

Examples

In this example, the command sets the operating mode of the default profile to **g992-1**:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile default
DSLAM(cfg-dsl-profile)# dmt operating-mode g992-1
```

Related Commands

Command	Description
dmt training-mode	Modifies the training mode in a DMT profile.

dmt overhead-framing

To set the overhead framing mode, use the **dmt overhead-framing** command.To reset this command to the default value, use the **no** form of this command.

dmt overhead-framing {**mode0** | **mode1** | **mode2** | **mode3**}

Syntax Description

mode0	Full overhead framing with asynchronous bit-to-modem timing.
mode1	Full overhead framing with synchronous bit-to-modem timing.
mode2	Reduced overhead framing with separate fast and sync bytes in the fast and interleaved latency buffers respectively.
mode3	Reduced overhead framing with merged fast and sync bytes, using either the fast or interleaved latency buffer.

Defaults

Mode3

Command Modes

Profile configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.1(6)DA	Mode 0 was added.

Usage Guidelines

Note Conditions on the line and the capabilities of the ATU-R CPE affect the achievable value for this parameter. As a result, the overhead framing value to which the line trains might not be the same as the value you configure.

There are two types of ADSL framing:

- Full overhead
- Reduced overhead

There are also two versions of full overhead:

- Asynchronous
- Synchronous

You select the type of ASDL framing by choosing one of four modes:

- Mode 0—Full overhead framing with asynchronous bit-to-modem timing (an enabled synchronization control mechanism).
- Mode 1—Full overhead framing with synchronous bit-to-modem timing (a disabled synchronization control mechanism).

- Mode 2—Reduced overhead framing with separate fast and sync bytes in the fast and interleaved latency buffers respectively.
- Mode 3—Reduced overhead framing with merged fast and sync bytes using either the fast or interleaved latency buffer.

Note Mode 3 is recommended for use on DMT interfaces that adhere to the ANSI T1.413 Issue 2 standard. Mode 3 is required for 4xflexi card DMT interfaces.

The number of overhead bytes per frame varies according to the overhead framing mode and the operating mode, as shown in Table 3-6.

Table 3-6 Overhead Bytes per Frame

	Overhead Bytes			
	T1.413 and G992.1		G992.2	
Framing Mode	Downstream	Upstream	Downstream	Upstream
Mode 0	4	3	—	—
Mode 1	3	3	—	—
Mode 2	2	2	—	—
Mode 3	1	1	1	1

If, during the training sequence, the ATU-R indicates a lower framing structure than that specified by the ATU-C, the ATU-C falls back to the framing structure number indicated by the ATU-R.

Management requirements drive the determination of overhead, full, or reduced. Full overhead provides more bandwidth to the embedded operations channel (EOC), enabling higher polling rates. However, reduced overhead provides enough bandwidth to satisfy typical applications.

If an ADSL line supports an ATM link, you must choose a structure that disables synchronization control. If an ADSL line is supporting an STM link and the ADSL line interface has a clock tightly coupled to the stratum clock, synchronization control is not necessary.

The **dmt overhead-framing** command does not cause port retrain when you change the parameter.

Examples

In this example, the command sets the overhead framing mode in the profile named 8xDMT.

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile 8xDMT
DSLAM(cfg-dsl-profile)# dmt overhead-framing mode2
```

Related Commands

Command	Description
show dsl profile [*profile name*]	Displays a specific profile or all profiles.

dmt power-management-additional-margin

To set power management mode for a DMT profile, use the **dmt power-management-additional-margin** command. To reset this command to the default value, use the **no** form of this command.

dmt power-management-additional-margin downstream *dmt margin* **upstream** *dmt margin*

Syntax Description

dmt-margin	Enter the upstream and downstream SNR margins in decibels. The range is 0 to 15.

Defaults

The default no dmt power-management-additional-margin sets both the downstream and upstream values to 0 dB. The following warning message appears when the power management feature is disabled by either the **no dmt power-management-additional-margin** command or by setting the values explicitly to 0dB: "warning: A 'power-management-additional-margin' value of 0dB disables the respective power management feature."

Command Modes

Profile configuration

Command History

Release	Modification
12.2(10)DA	This command was introduced.

Usage Guidelines

The 8xDMT line card can run in power-management mode in the G.dmt or the T1.413 mode. The resulting power cutback produces a reduction in power dissipation and crosstalk. Only 8xDMT line cards support power management. All CPE may not support the DSL functionality for power management to function correctly. Check with a Cisco customer representative to verify CPE compatibility with the 8xDMT power management feature.

You control the Power Management feature by issuing a **dmt power-management-additional-margin** command inside a profile and assigning that profile to a line card interface. This IOS command allows you to set the additional margin for each channel from 0 dB (off) to 15 dB. This sets the additional margin that will be added to the target margin. If the sum of the target margin and additional margin exceeds 15dB, it is capped at 15dB. If the actual margin of the line is higher than the sum of the configured target and additional margin, and all the above conditions are met, then power management attempts to reduce the actual margin, and as a consequence the power level as well.

Not all CPE support power management. If you connect an unsupported CPE to a port on which power management is turned on, you will not see a reduction in the actual margin or power level. The operating modes supported by power management are T1.413and g-992-1 (g.dmt). A reduction in the power level occurs if there is excess margin on the line. For the downstream direction, if there is excess margin, then IOS displays a reduction in margin for the modes listed above, and a reduction in transmit power for T1.413 mode. For the upstream direction, if there is excess margin, then IOS displays a reduction in the margin for g-992-1 mode only. IOS will not display a reduction in transmit power for the upstream direction.

The following warning message appears when you enable the power management feature:

```
"warning: If sum of 'power-management-additional-margin' and the configured 'margin'
exceeds 15dB, the resulting value will be capped at 15dB."
```

Examples

In the following example, power management would begin at 9dB because the orginal margin is 6dB and the additional margin is 3dB:

```
DSLAM# config terminal
DSLAM(config)# dsl-profile austin
DSLAM(cfg-dsl-profile)# dmt margin downstream 6 upstream 6
DSLAM(cfg-dsl-profile)# dmt power-management-additional-margin downstream 3 upstream 3
```

Related Commands

Command	Description
dmt margin	Sets upstream and downstream signal-to-noise ratio (SNR) margins for a DMT profile.

dmt rate-adaptation enable

DMT rate adaptation monitors upstream and downstream DMT ports for signal-to-noise ratio (SNR) margins during specified time intervals. If the system detects an unacceptable SNR margin and that margin persists for the specified time interval, the port retrains at a lower bit rate to improve the SNR margins. To enable rate adaptation on a DMT port, use the **dmt rate-adaptation enable** command at the DSL profile configuration prompt. To disable dmt rate adaptation, use the **no** form of the command.

dmt rate-adaptation enable

Syntax Description

This command has no arguments or keywords.

Defaults

Enabling dmt rate-adaptation configures the **dmt rate-adaptation interval** and **dmt rate-adaptation margin** commands with their default values. For information on the default values of **dmt rate-adaptation interval** and **dmt rate-adaptation margin**, see the "dmt rate-adaptation interval" section on page 3-48 and the "dmt rate-adaptation margin" section on page 3-50.

Command Modes

DSL profile configuration

Command History

Release	Modification
12.1(6)DA	This command was introduced.

Usage Guidelines

If you want to modify the default configuration of the **dmt rate-adaptation interval** and **dmt rate-adaptation margin** commands, see the "dmt rate-adaptation interval" section on page 3-48 and the "dmt rate-adaptation margin" section on page 3-50.

Examples

The following example enables **dmt rate-adaptation** with default interval and margin values:

```
DSLAM# config terminal
DSLAM(config)# dsl-profile austin
DSLAM(cfg-dsl-profile)# dmt rate-adaptation enable
```

Related Commands

Command	Description
dmt rate-adaptation interval	Sets the upstream and downstream time intervals during which a DMT port is monitored for SNR margins.
dmt rate-adaptation margin	Sets the SNR values below which the DMT port retrains to a lower bit rate.

dmt rate-adaptation interval

To change the intervals during which a DMT port is monitored for signal-to-noise ratio (SNR) margins, use the **dmt rate adaptation interval** command in DSL profile configuration mode. To disable **dmt rate adaptation interval**, use the **no** form of this command.

dmt rate-adaptation interval {downshift [downstream *number-of eoc-updates* **upstream** *seconds***]}**

Syntax Description

downshift	Indicates that a line with excessive SNR margins retrains to a lower bit rate.
downstream	Tells Cisco IOS to monitor downstream ports for SNR margins that exceed those specified in the **dmt rate-adaptation margin** command.
number-of eoc-updates	Specifies the monitoring interval on a downstream DMT port. **Note** The downstream margin (see the "dmt rate-adaptation margin" section on page 3-50) is obtained from the CPE via the embedded operations channel (EOC). The **downstream** *number-of eoc-updates* parameter specifies a number of consecutive EOC read events. Depending on the type of CPE, EOC messages are sent once every 6 to 15 seconds (not counting EOC timeouts). Therefore, a downstream downshift interval value of 10 on CPE reporting margins every 6 seconds results in a 1-minute monitoring interval (10 x 6 seconds). Specifying a downstream downshift interval value of 10 on a CPE that reports margins every 15 seconds (10 x 15 seconds) yields a 2.5-minute monitoring interva1.
upstream	Tells Cisco IOS to monitor upstream ports for SNR margins that exceed those specified in the **dmt rate-adaptation margin** command.
seconds	Specifies the monitoring interval in seconds on an upstream DMT port.

Defaults

The following default settings are for the **dmt rate-adaptation interval**:

- Downstream—10

Note Remember that a downstream value of 10 can yield a monitoring interval between 1 minute and 2.5 minutes in length.

- Upstream—10

Command Modes

DSL profile configuration

Command History

Release	Modification
12.1(6)DA	This command was introduced.

Usage Guidelines

Use the **dmt rate-adaptation interval** command to specify the duration over which line margins are checked on a DMT port. The **dmt rate-adaptation interval** command works in conjunction with the **dmt rate-adaptation margin** command. If the actual SNR margins on a port remain lower than the margins configured in the **dmt rate-adaptation margin** command, for the duration of time specified in the **dmt rate-adaptation interval** command, the line drops and retrains to a lower bit rate, to improve SNR margin quality on the line.

Note If line conditions improve, the line does not automatically drop and retrain to a higher bit rate. If the line conditions improve, the administrator must execute a **shutdown** and then a **no shutdown** on the port to retrain to a higher bit rate.

Examples

The following example configures a downstream monitoring interval of roughly 60 to 150 seconds. The upstream monitoring interval is 20 seconds.

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile austin
DSLAM(cfg-dsl-profile)# dmt rate-adaptation interval downshift downstream 10 upstream 20
```

Related Commands

Command	Description
dmt rate-adaptation enable	Turns on rate adaptation.
dmt rate-adaptation margin	Sets the SNR margins below which a DMT port retrains to a lower bit rate.

dmt rate-adaptation margin

To configure the minimum acceptable SNR margins on a DMT port, which forces the port to retrain when unacceptable margins exist for the duration of the **dmt rate-adaptation interval,** use the **dmt rate-adaptation margin** command in DSL profile configuration mode. To disable the dmt rate adaptation margin, use the **no** form of this command.

dmt rate-adaptation margin {min [downstream *dB* **upstream** *dB*]}

Syntax Description

min	Use the **min** keyword to configure the minimum acceptable SNR margins on a port. If the port SNR exceeds the configured value, the port retrains to a lower bit rate.
downstream	The minimum acceptable SNR margin for downstream traffic on a port.
dB	SNR margins measured in decibels. The valid range is –15 to 15.
upstream	The minimum acceptable SNR margin for upstream traffic on a port.
dB	SNR margins measured in decibels. The valid range is –15 to 15.

Defaults

The default configuration is derived from the **no dmt rate-adaptation enable** command. This command specifies minimum upstream and downstream SNR margins of 0 dB.

Command Modes

DSL profile configuration

Command History

Release	Modification
12.1(6)DA	This command was introduced.

Usage Guidelines

Use the **dmt rate-adaptation margin** command to configure the acceptable SNR margin thresholds on a specified port. The **dmt rate-adaptation margin** command works in conjunction with the **dmt rate-adaptation interval** command. If the actual SNR margins on a port remain lower than the margins configured in the **dmt rate-adaptation margin** command, for the duration of time specified in the **dmt rate-adaptation interval** command, the line drops and retrains to a lower bit rate, to improve SNR margin quality on the line.

Note If line conditions improve, the line does not automatically drop and retrain to a higher bit rate. If the line conditions improve, the administrator must execute a **shutdown** and then a **no shutdown** on the affected port to retrain to a higher bit rate.

Defaults

The following example describes how to configure **dmt rate-adaptation margin**:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile austin
DSLAM(cfg-dsl-profile)# dmt rate-adaptation margin min downstream 10 dB upstream -10
```

Related Commands

Command	Description
dmt rate-adaptation enable	Turns on rate adaptation.
dmt rate-adaptation interval	Configures the intervals at which DMT ports are monitored for substandard SNR margins.

dmt training-mode

To modify the training mode in a DMT profile, use the **dmt training-mode** command in profile configuration mode. To set the training mode in a DMT profile to the default setting (quick), use the **no** form of the command.

dmt training-mode {**standard** | **quick**}

no dmt training-mode

Syntax Description

standard	Depending on the configuration, standard training uses either the T1.413-1998 or the G.994.1 initialization method. In standard training mode, the ATU-C line card trains the modem once. If the configured rates and settings are not obtainable, the line card reads the line quality and retrains, selecting the best available rates and settings. The line card software determines the best available rates. This mode allows more control over the DMT parameters.
quick	This training mode uses either the extended exchange sequence for T1.413-1998 initialization or the G.994.1 initialization, depending on the configuration. In quick training mode the modem DSP automatically chooses the best available rate based on the parameters provided. The DSP might be forced to change some of the configuration settings based on line characteristics. This training mode is faster than the standard training mode.

Note This command applies to the 4xDMT card only. A 4xflexi line card configured for DMT uses quick training all the time.

Defaults

Quick

Note We recommend that you use quick-training mode on all interfaces. Standard training mode is not supported on 4xflexi line cards.

Command Modes

Profile configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

Quick-training mode is recommended for all interfaces.

Caution This command causes the port to retrain when you change the training mode parameter.

Examples

In this example, the command sets the training mode of the default profile to standard:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile default
DSLAM(cfg-dsl-profile)# dmt training-mode standard
```

Related Commands

Command	Description
dmt operating-mode	Modifies the operating mode of a line in the DSL profile.

dns-server

To specify the Domain Name System (DNS) IP servers that are available to a Dynamic Host Configuration Protocol (DHCP) client, use the **dns-server** DHCP pool configuration command. Use the **no** form of this command to remove the DNS server list.

dns-server *address* [*address2 ... address8*]

no dns-server

Syntax Description

address	Specifies the IP address of a DNS server. One IP address is required, although you can specify up to eight addresses in one command line.

Defaults

If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

Servers are listed in order of preference (address1 for the most preferred server, address2 for the next most preferred server, and so on).

Examples

The following example specifies 10.12.1.99 as the IP address of the domain name server of the client:

```
DSLAM(config)# ip dhcp pool 1
DSLAM(dhcp-config)# dns-server 10.12.1.99
```

Related Commands

Command	Description
domain-name	Specifies the domain name for a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

domain-name

To specify the domain name for a Dynamic Host Configuration Protocol (DHCP) client, use the **domain-name** DHCP pool configuration command. Use the **no** form of this command to remove the domain name.

domain-name *domain*

no domain-name

Syntax Description

domain	Specifies the client domain name string.

Defaults

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Examples

The following example specifies cisco.com as the domain name of the client:

```
DSLAM(config)# ip dhcp pool 1
DSLAM(dhcp-config)# domain-name cisco.com
```

Related Commands

Command	Description
dns-server	Specifies the Domain Name System (DNS) IP servers available to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

dsl atuc-1-4dmt rx-attenuation

The **dsl atuc-1-4dmt rx-attenuation** global configuration command turns on a received power attenuator in all of the 4xDMT line cards in a chassis. This command also automatically retrains all the ports on all of the 4xDMT line cards.

dsl atuc-1-4dmt rx-attenuation

Syntax Description

This command has no arguments or keywords.

Defaults

dsl atuc-1-4dmt rx-attenuation

Command Modes

Global configuration

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Usage Guidelines

You can determine the state of this setting by using the **show running-config** command to check for **no dsl atuc-1-4dmt rx-attenuation**. The default setting, dsl atuc-1-4dmt rx-attenuation, is not displayed by **show running-config**.

Examples

In this example, the received power attenuator in all of the 4xDMT line cards in a chassis is turned off.

```
DSLAM# configure terminal
DSLAM(config)# no dsl atuc-1-4dmt rx-attenuation
```

Related Commands

Command	Description
show running-config	Displays the running configuration for every currently defined profile, including the default.

dsl circuit

To assign an identifier to a DSL circuit, use the **dsl circuit** interface configuration command. To remove an identifier from a DSL circuit (that is, to leave the field blank), use the **no** form of the command.

dsl circuit *circuit-id*

no dsl circuit

Syntax Description

circuit-id	The identifier that you assign to the circuit. The circuit ID can contain up to 32 printable characters. Alphanumerics and most special characters (underscores, hyphens, and ampersands, for example) are allowed. Spaces and quotes are not allowed.

Defaults

There is no default value for this command.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.1(1)DA	DSL circuit identifier capability was added.

Usage Guidelines

If different circuit identifiers are assigned to the same interface, the latest assigned circuit ID takes precedence. You can modify an identifier to a DSL circuit by assigning a different circuit ID to the same interface.

Examples

In this example, the circuit ID 341 is assigned to slot 7, port 3.

```
DSLAM# configure terminal
DSLAM(config)# interface atm 7/3
DSLAM(config-if)# dsl circuit 341
```

Related Commands

Command	Description
dsl subscriber	Assigns a name to a DSL port.
show dsl interface atm *slot#/port#*	Displays DSL and ATM status for a port.
show dsl status	Displays the status of the DSL subscriber ports on a chassis.
show running-config	Displays the running configuration for every currently defined profile.

dsl-copy-profile

To copy a DSL profile, use the **dsl-copy-profile** command.

dsl-copy-profile [**force**] **source** *source-profile* **destination** *new-profile*

Syntax Description

force	Overwrite the destination file, if it exists.
source-profile	The profile whose information you want to copy to another profile.
new-profile	The destination profile.

Defaults

There is no default value for this command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.1(1)DA	The capability to create a copy of an SDSL profile was added.

Usage Guidelines

If the destination profile indicated in this command does not exist, **dsl-copy-profile** creates it. The command then copies all configuration values in the source profile to the destination profile.

Note If you modify the source profile after you issue this command, the changes you make do not propagate to the destination profile.

Examples

This command copies the default profile to a profile named my_default. If my_default does not exist, the command creates it.

```
DSLAM# configure terminal
DSLAM(config)# dsl-copy-profile force source default destination my_default
```

Related Commands

Command	Description
dsl-profile	Creates a DSL profile or selects an existing profile for modification.
show dsl profile [*profile name*]	Displays a specific profile or all profiles.
show running-config	Displays the running configuration for every currently defined profile, including the default.

dsl-profile

To create a DSL profile, or to select an existing profile for modification, use the **dsl-profile** command in global configuration mode. To delete a DSL profile, use the **no** form of the command.

dsl-profile *profile-name*

no dsl-profile *profile-name*

Note Cisco IOS includes two very similar commands, **dsl-profile** (in global configuration mode) and **dsl profile** (in interface configuration mode). The **dsl-profile** command creates a DSL profile, and the **dsl profile** command attaches a port to an existing DSL profile. Be sure you use the correct command for your purpose.

Syntax Description

profile-name	The name of the profile you want to create, or an existing profile you want to delete or modify.

Defaults

Initially, every newly created profile has the system defined default values.

Note You cannot delete the default profile or any profile that is attached to a port. However, you can modify the default profile.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

A profile is a named list of configured items. To configure a subscriber, you must attach a profile to that subscriber port. You can change the configured items for a subscriber by changing that subscriber profile.

You configure a port by using a configuration profile, rather than by direct configuration.

If you modify an existing profile, the change that you make takes effect on every ADSL port linked to that profile.

When you use the **dsl-profile** command, you might create a new profile with system-defined default values. The system automatically names this new profile “default.”

If you change the default profile, the change does not propagate to the children of that default profile.

This configuration profile approach is in keeping with ADSL MIB standards.

Examples

This command implicitly creates a DSL profile named example, if it does not already exist. After you execute the steps shown here, you can modify the parameters for this profile:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile example
DSLAM(cfg-dsl-profile)#
```

In this example, the command modifies the default profile:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile default
DSLAM(cfg-dsl-profile)#
```

Related Commands

Command	Description
dsl-copy-profile	Copies a DSL profile.
dsl profile	Attaches a profile to a specific port.
show dsl profile [*profile name*]	Displays a specific profile or all profiles.
show running-config	Displays the running configuration for every currently defined profile, including the default.

dsl profile

To attach a port to a profile, use the **dsl profile** command in interface configuration mode. To detach the port from its profile and attach the default profile, use the **no** form of the command.

dsl profile [*profile-name***]**

no dsl profile

Note Cisco IOS includes two very similar commands, **dsl-profile** (in global configuration mode) and **dsl profile** (in interface configuration mode). Be sure you are using the correct command for your purpose.

Syntax Description

profile-name	The profile you want to attach to the selected port.

Defaults

By default, every port is attached to a special profile named "default."

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

A profile is a named list of configured items. To configure a subscriber, you must attach a profile to that subscriber port. You can change the configured items for a subscriber by changing that subscriber profile.

Except for a few dynamic operational modes, port configuration takes place through a configuration profile, rather than by direct configuration.

If you modify an existing profile, the change that you make takes effect on every ADSL port linked to that profile.

This configuration profile approach is in keeping with ADSL MIB standards.

The DSLAM implementation uses the dynamic profile approach, as opposed to the static profile approach. The dynamic profile approach supports a many-to-one correspondence between ports and profiles; that is, there can be one profile for many ports, but one port cannot have more than one profile. Also, with the dynamic approach, profiles are created and deleted dynamically (with the exception of a special profile named default). Direct configuration of port parameters is not allowed.

All ports have attached profiles. If you do not assign a profile to a port, the system, by default, assigns the profile named "default."

Examples

In this example, the command attaches the profile test1 to slot 20, port 1:

```
DSLAM# configure terminal
DSLAM(config)# interface atm 20/1
DSLAM(config-if)# dsl profile test1
```

Related Commands

Command	Description
dsl-copy-profile	Copies a DSL profile.
dsl-profile	Creates a DSL profile or selects an existing profile for modification.
show dsl profile [*profile name*]	Displays a specific profile or all profiles.
show dsl interface atm	Displays DSL and ATM status for a port.
show running-config	Displays the running configuration for every currently defined profile, including the default.

dsl subscriber

To assign a name to a DSL port, use the **dsl subscriber** command in interface configuration mode. To remove a name from a port (that is, to leave the field blank), use the **no** form of the command.

dsl subscriber *name*

no dsl subscriber

Syntax Description

name	The string that you define as the name of the port. The string can contain up to 64 printable characters. Alphanumerics and most special characters (underscores, hyphens, and ampersands, for example) are allowed. Spaces and quotes are not allowed.

Defaults

There is no default value for this command.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

You can use the port name to identify the subscriber the port serves. You can modify the port name by assigning a different name to the same port; the latest assigned name takes precedence.

Examples

In this example, the name paul is assigned to slot 7, port 3.

```
DSLAM# configure terminal
DSLAM(config)# interface atm 7/3
DSLAM(config-if)# dsl subscriber paul
```

Related Commands

Command	Description
dsl circuit	Assigns an identifier to a DSL circuit.
show dsl interface atm *slot#/port#*	Displays DSL and ATM status for a port.
show dsl status	Displays the status of the DSL subscriber ports on a chassis.
show running-config	Displays the running configuration for every currently defined profile.

dsl test atm self

To run the line card port self-test, use the command

dsl test atm *slot#/port#* **self**

Syntax Description

slot#/port#	The slot and port numbers for which you want to run the line card chipset self-test. The slot range is 1 to 38. The port range is 1 to 8. (These are maximum ranges; your card might have fewer than 8 ports and your chassis might have fewer than 38 slots.)

Defaults

There is no default value for this command.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

This command runs a digital bit error-rate loopback test on the specified port. The run time for the self-test ranges from 3 seconds for the ATUC-1-4DMT card to 1 minute for the 4xflexi card.

To view the result of the self-test, use the command **show dsl interface atm** *slot#/port#*.

The output display for this command includes the result of the last self-test, such as

```
Last Self-Test Result: NONE
```

The possible self-test results are PASSED, FAILED, RUNNING, and NONE.

The NONE result means that a chipset self-test has not run since the port became operational.

RUNNING means the test is in progress.

Caution The line card port self-test disrupts port operation. If a port has been trained or is training when this test begins, the port becomes untrained, the test executes, and the port retrains.

Examples

In this example, the command runs the self-test for port 1 in slot 20:

```
DSLAM# dsl test atm 20/1 self
```

Related Commands

Command	Description
show dsl interface atm	Displays DSL and ATM status for a port.

E Through M Commands for Cisco DSLAMs with NI-2

This chapter documents commands that you use to configure Cisco DSLAMs with NI-2. Commands in this chapter are listed alphabetically. For information on how to configure DSL features, refer to the *Configuration Guide for Cisco DSLAMs with NI-2*.

Note Commands that are identical to those documented in the *Cisco IOS Configuration Fundamentals Command Reference* and the *ATM and Layer 3 Switch Router Command Reference* have been removed from this chapter.

This chapter discusses the following commands:

encapsulation

exit-address-family

framing

hardware-address

host

ima active-links-minimum

ima clock-mode

ima differential-delay-maximum

ima frame-length

ima-group

ima test

ima version

import map

ip cef traffic-statistics

ip classless

ip default-gateway

ip dhcp conflict logging

ip dhcp database

ip dhcp excluded-address

ip dhcp ping packets

ip dhcp ping timeout

ip dhcp pool

ip dhcp relay information option

ip helper-address

ip local pool

ip route vrf

ip routing

ip subnet-zero

ip unnumbered

ip vrf

ip vrf forwarding

lbo

lease

linecode

loopback

encapsulation

To set the encapsulation method that the interface uses , use the **encapsulation** interface configuration command.

encapsulation *encapsulation-type*

Syntax Description

encapsulation-type	Encapsulation type. See Table 4-1 for a list of supported encapsulation types.

Defaults

The default depends on the type of interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

For you to use SLIP or PPP, the router or access server must be configured with an IP routing protocol or with the **ip host-routing** command. This configuration is done automatically if you are using old-style SLIP address commands. However, you must configure manually if you configure SLIP or PPP with the interface async command.

Table 4-1 Supported Encapsulation Types

Keyword	Encapsulation Type
aal5ciscoppp	Cisco PPP over AAL5 encapsulation.
aa15mux	AAL5+MUX encapsulation.
aal5nlpid	AAL5+NLPID encapsulation. **Note** AAL5+NLPID encapsulation is not applicable to configuring the DSLAM.
aa15snap	AAL5+LLC/SNAP encapsulation.

The following example enables aal5snap encapsulation on atm interface 1/1:

```
DSLAM#conf t
DSLAM(config)#interface atm0/1
DSLAM(config-if)#atm pvc 0 100 interface atm 0/0 0 100 encap aal5snap
```

Related Commands

Command	Description
ppp authentication	Enables Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) and enables an AAA authentication method on an interface.

exit-address-family

To exit from the address-family submode, use the **exit-address-family** address-family submode command.

exit-address-family

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Address-family submode

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

You can abbreviate this command to **exit**.

Examples

The following example shows how to exit the address-family command mode:

```
DSLAM# configure terminal
DSLAM(config)# router bgp 100
DSLAM(config-router)# address-family ipv4 unicast vrf vrf2
DSLAM(config-router-af)# exit-address-family
```

Related Commands

Command	Description
address-family	Enters the address-family submode that you use to configure routing protocols.

framing

To select the frame type for the data link, use the **framing** interface configuration command. To restore the default values, use the **no** form of this command.

framing *framingmode*

Syntax Description

framingmode	Specify *framingmode* as follows: • For E1: **pcm30** | **crc4** • For E3: **g751adm** | **g751plcp** | **g832adm** • For T1: **esf** | **sf** • For DS3: **cbitadm** | **cbitplcp** | **m23adm** | **m23plcp**

Defaults

For E1: **pcm30**

For E3: **g832adm**

For T1: **esf**

For DS3: **cbitadm**

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

In the E1 environment, the **framing** command allows selection of the E1 frame type to CRC4 enabled framing mode (**crc4**) or CRC4 disabled framing mode (**pcm30**).

In the E3 environment, the **framing** command allows the selection of the E3 frame type to g751 ADM, g751 PLCP, or g832 ADM.

In the T1 environment, the **framing** command allows selection of the T1 frame type to extended super frame (**esf**) or super frame (**sf**).

In the DS3 environment, the **framing** command allows the selection of the DS3 frame type to C-Bit ADM, C-Bit PLCP, M23 ADM, or M23 PLCP.

Note The framing type must match on both sides of a link.

Examples

The following example shows how to select **m23plcp** as the frame type:

```
DSLAM(config)# interface atm 0/1
DSLAM(config-if)# framing m23plcp
```

Related Commands

Command	Description
show controllers	Displays information about a physical port device.

hardware-address

To specify the hardware address of a Dynamic Host Configuration Protocol (DHCP) client, use the **hardware-address** DHCP pool configuration command. This command is valid for manual bindings only. Use the **no** form of this command to remove the hardware address.

hardware-address *hardware-address type*

no hardware-address

Syntax Description

hardware-address	Specifies the MAC address of the client hardware platform.
type	Indicates the protocol of the hardware platform. Strings and values are acceptable. The string options include: ethernet ieee802 The value options include: 1 10Mb Ethernet 6 IEEE 802 If no type is specified, the default protocol is Ethernet.

Defaults

Ethernet is the default type if if you do not specify one.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Examples

The following example specifies b708.1388.f166 as the MAC address of the client:

```
DSLAM(config)# ip dhcp pool 1
DSLAM(dhcp-config)# hardware-address b708.1388.f166
```

Related Commands

Command	Description
client-identifier	Specifies a unique identifier for a DHCP client.
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

host

To specify the IP address and network mask for a manual binding to a Dynamic Host Configuration Protocol (DHCP) client, use the **host** DHCP pool configuration command. Use the **no** form of this command to remove the client IP address.

host *address* [*mask* | */prefix-length*]

no host

Syntax Description

address	Specifies the IP address of the client.
mask	(Optional) Specifies the network mask of the client.
/prefix-length	(Optional) Specifies the number of bits that make up the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/).

Defaults

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

If you do not specify the mask and prefix length, DHCP examines its address pools. If the software fails to find a mask in the pool database, it uses the Class A, B, or C natural mask. This command is valid for manual bindings only.

Examples

The following example specifies 10.12.1.99 as the client IP address and 255.255.248.0 as the subnet mask:

```
DSLAM#conf t
DSLAM(config)#ip dhcp pool test
DSLAM(dhcp-config)# host 10.12.1.99 255.255.248.0
```

Related Commands

Command	Description
client-identifier	Specifies a unique identifier for a DHCP client.
hardware-address	Specifies the hardware address of a DHCP client.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.

ima active-links-minimum

To configure the minimum number of active links required for an IMA group to function, use the **ima active-links-minimum** interface configuration command. To restore the default value, use the **no** form of this command.

ima active-links-minimum *number*

no ima active-links-minimum

Syntax Description

number	Minimum number (1 to 8) of active links for an IMA group to function.

Defaults

No minimum links is the default (**no ima active-links-minimum** or **ima active-links-minimum 1**).

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

This command sets the minimum number of links that must be in the active state before the IMA group interface becomes active. If at any time the number of active links is less than this value, the IMA group interface will no longer be active.

Examples

The following example uses the **ima active-links-minimum** command to configure the minimum number of active links that must be active for the IMA group to function correctly:

```
DSLAM(config)# interface atm 0/ima0
DSLAM(config-if)# ima active-links-minimum 2
```

Related Commands

Command	Description
show ima interface	Displays information about all IMA groups and the links in those groups.
show ima interface atm0/ima *group-number*	Displays information about a single IMA group and the links in that group.

ima clock-mode

To set the transmit clock mode for an ATM IMA group, use the **ima clock-mode** interface configuration command. To restore the default value, use the **no** form of this command.

ima clock-mode {common {2-9} | independent}

no ima clock-mode

Syntax Description

common	Group with a link number that is used as a common clock source for all other links in the IMA group. If the specified link is not available, another link in the group is used until the specified link is added.
independent	Group so that each link in the group is clocked independently based on its own clock source setting.

Defaults

By default, the first link added to the group is used as the common clock source (**ima clock-mode common**).

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

This command controls the clock for the IMA group as a whole. When you set the **independent** keyword, the **clock source** interface configuration command is used under each interface to determine clocking individually. When you set the **common** keyword, the **clock source** interface configuration command for the common link determines clocking for all the links in the group.

Note The IMA clock mode must match on both sides of an IMA link.

Examples

The following example uses the **ima clock-mode** command to configure the IMA group clocking mode as independent:

```
DSLAM(config)# interface atm 0/ima0
DSLAM(config-if)# ima clock-mode independent
```

Related Commands

Command	Description
clock source	Selects the transmit clock source for a link.

ima differential-delay-maximum

To specify a maximum differential timing delay among the links in an IMA group, use the **ima differential-delay-maximum** interface configuration command. If a link delay exceeds the specified maximum, the link drops; otherwise, the IMA feature, while multiplexing and demultiplexing, adjusts for differences in delays to align all links in a group. The **no** form of the command restores the default setting.

ima differential-delay-maximum {*msecs***}**

no ima differential-delay-maximum

Syntax Descriptionn

msecs	Maximum differential delay in milliseconds as follows: • For T1 the range is 25 to 281 milliseconds. • For E1 the range is 25 to 225 milliseconds.

Defaults

The default is 25 milliseconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

The transmitter on the T1/E1 IMA port adapter must align the transmission of IMA frames on all interfaces that are members of the IMA group. This alignment allows the receiver to adjust for differential link delays among the interfaces that are members of the IMA group. Based on this required behavior, the receiver can detect the differential delays by measuring the arrival times of the IMA frames on each link.

At the transmitting end, the cells transmit continuously. If no ATM layer cells need to transmit between IMA control protocol (ICP) cells with an IMA frame, then the transmit IMA sends filler cells to maintain a continuous stream of cells at the physical layer.

Examples

The following example configures the maximum allowable differential delay to 55 milliseconds for all interfaces assigned to the IMA group:

```
DSLAM(config)# interface atm 0/ima0
DSLAM(config-if)# ima differential-delay-maximum 55
```

Related Commands

Command	Description
show ima interface	Displays information about all IMA groups and the links in those groups.
show ima interface atm0/ima *group-number*	Displays information about a single IMA group and the links in that group.
show ima interface atm0/*interface-number*	Displays information for a single link in an IMA group including delay on that link.

ima frame-length

To set the IMA frame length in cells per frame, use the **ima frame-length** interface configuration command.

ima frame-length {32 | 64 | 128 | 256}

no ima frame-length

Syntax Description

32	Configure IMA frame length to 32 cells.
64	Configure IMA frame length to 64 cells.
128	Configure IMA frame length to 128 cells (default).
256	Configure IMA frame length to 256 cells.

Defaults

The default is 128 cells.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

An IMA group uses the frame length parameter to set the insertion of the IMA control protocol (ICP) cells at the beginning of frames in the transmit direction. Normally, one ICP cell is sent per IMA frame. The larger the IMA frame, the less overhead there is at the expense of a decrease in allowable timing differences between the lengths.

Examples

The following example uses the **ima frame-length** command to configure the frame length that is transmitted as 64 cells for the IMA group:

```
DSLAM(config)# interface atm 0/ima0
DSLAM(config-if)# ima frame-length 64
```

Related Commands

Command	Description
show ima interface	Displays information about all IMA groups and the links in those groups.

ima-group

To assign a T1/E1 link to an IMA group, use the **ima-group** interface configuration command. The **ima-group** interface configuration command applies only to atm 0/2 through atm 0/9 (see Table 2-3 on page 2-26).To remove a link from an IMA group, use the **no** form of this command.

ima-group *number*

no ima-group

Syntax Description

number	IMA group number (0 to 3).

Defaults

The links do not belong to any IMA group by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

Use the **ima-group** interface command to configure a T1/E1 port adapter interface as part of an IMA group. IMA allows you to aggregate multiple low-speed links into one larger virtual trunk or IMA group. This IMA group appears to your ATM switch router as one logical pipe. It also provides modular bandwidth for user access to ATM networks for connections between ATM network elements that are at rates between traditional multiplexing levels, such as between T1/E1, and DS3/E3.

IMA requires inverse multiplexing and demultiplexing of ATM cells in a cyclical fashion among links that are grouped to form a higher-bandwidth logical group with a rate of approximately the sum of the link rates. This grouping is called an IMA group.

Examples

The following example uses the **ima-group** command to assign link 0 to IMA group 0:

```
DSLAM(config)# interface atm 0/2
DSLAM(config-if)# ima-group 0
```

Related Commands

Command	Description
show controllers	Displays information about a physical port device.
show ima interface	Displays information about all IMA groups and the links in those groups.
show ima interface atm0/ima *group-number*	Displays information about a single IMA group and the links in that group.

ima test

To configure an IMA group test pattern transmitted in the ICP cells, use the **ima test** interface configuration command. To restore the default value, use the **no** form of this command.

ima test [link *link-value***] [pattern** *pattern-value***]**

no ima test

Syntax Description

link	Link that transmits the test pattern.
link-value	The IMA group member link (2 through 9) that transmits the test pattern.
pattern	Test pattern.
pattern-value	Test pattern (0 through 255) transmitted in the ICP cells.

Defaults

The link-value is 2.

The pattern-value is 166.

The default is **no ima test**.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

The test pattern procedure verifies the connectivity of a link within an IMA group. The procedure uses a test pattern that it sends over one link to verify the connectivity to the other links in the IMA group. Ensure that the test pattern loops over all the other links in the group at the far end of the connection. The system performs all of the IMA test pattern procedures over the ICP cells that are exchanged between both ends of the IMA virtual links. After you configure the test on the IMA group, the test continues explicitly until you issue the **no** form of the command.

Examples

The following example uses the **ima test** command to configure the test pattern of 100 to transmit over ATM interface 0 of IMA group 0:

```
DSLAM(config)# interface atm 0/ima0
DSLAM(config-if)# ima test link 2 pattern 100
```

Related Commands

Command	Description
show ima interface	Displays information about all IMA groups and the links in those groups.

ima version

To set the operating mode of an IMA group, use the **ima version** interface configuration command. To restore the default value, use the **no** form of this command.

ima version {1.0 | 1.1}

no ima version

Syntax Description

1.0	The group runs in version 1.0 mode.
1.1	The group runs in version 1.1 mode.

Defaults

The default is version 1.0 mode.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Examples

The following example uses the **ima version** command to set the IMA version to 1.1:

```
DSLAM(config)# interface atm 0/ima0
DSLAM(config-if)# ima version 1.1
```

Related Commands

Command	Description
show ima interface	Displays information about all IMA groups and the links in those groups.
show ima interface atm0/ima *group-number*	Displays information about a single IMA group and the links in that group.

import map

To configure an import route map for a VPN routing/forwarding instance (VRF), use the **import map** VRF submode command.

import map *route-map*

Syntax Description

route-map	Route map to use as an import route map for the VRF.

Defaults

There is no default. A VRF has no import route map unless you configure one by using the **import map** command.

Command Modes

VRF submode

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

Use an import route map when you require control over the routes that you import into a VRF that is finer than the control provided by the import and export extended communities that are configured for the importing and exporting VRF.

The **import map** command associates a route map with the specified VRF. You can filter routes that are eligible for import into a VRF, based on the route target extended community attributes of the route, through the use of a route map.

Examples

The following example shows how to configure an import route map for a VRF:

```
DSLAM(config)# ip vrf vrf_blue
DSLAM(config-vrf)# import map blue_import_map
```

Related Commands

Command	Description
ip vrf	Enters VRF configuration mode.
route-target	Configures import and export extended community attributes for the VRF.
show ip vrf	Displays information about a VRF or all VRFs.

ip cef traffic-statistics

To change the time interval that controls when Next Hop Resolution Protocol (NHRP) will set up or tear down a switched virtual circuit (SVC), use the **ip cef traffic-statistics** global configuration command. To restore the default values, use the **no** form of this command.

ip cef traffic-statistics [**load-interval** *seconds*] [**update-rate** *seconds*]

no ip cef traffic-statistics

Syntax Description

load-interval *seconds*	(Optional) Length of time (in 30-second increments) during which the average *trigger-threshold* and *teardown-threshold* are calculated before an SVC setup or teardown action is taken. The **load-interval** range is 30 to 300 seconds, in 30-second increments. The default value is 30 seconds.
update-rate *seconds*	(Optional) Frequency with which the port adapter sends the accounting statistics to the resolution protocol. When you use NHRP in distributed CEF switching mode, you must set this value to 5 seconds. The default value is 10 seconds.

Defaults

load-interval: 30 seconds

update-rate: 10 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

To change the interval, use the **load-interval** *seconds* argument of the **ip cef traffic-statistics** command.

Examples

In the following example, the triggering and teardown thresholds are calculated based on an average over 120 seconds:

```
DSLAM(config)# ip cef traffic-statistics load-interval 120
```

Related Commands

Command	Description
ip nhrp trigger-svc	Configures when NHRP will set up and tear down an SVC based on aggregate traffic rates.

ip classless

At times the router might receive packets destined for a subnet of a network that has no network default route. To have the Cisco IOS software forward such packets to the best supernet route possible, use the **ip classless** global configuration command. To disable this feature, use the **no** form of this command.

ip classless

no ip classless

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

This command allows the software to forward packets that are destined for unrecognized subnets of directly connected networks. The packets are forwarded to the best supernet route.

When this feature is disabled, the software discards the packets for a subnet that numerically falls within its subnetwork addressing scheme. If there is no such subnet number in the routing table, there is no network default route.

Examples

The following example prevents the software from forwarding packets that are destined for an unrecognized subnet to the best supernet possible:

```
DSLAM(config)# no ip classless
```

Related Commands

None.

ip default-gateway

To define a default gateway (router) when IP routing is disabled, use the **ip default-gateway** global configuration command. To disable this function, use the **no** form of this command.

ip default-gateway *ip-address*

no ip default-gateway *ip-address*

Syntax Description

ip-address	IP address of the router.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The Cisco IOS software sends any packets that need the assistance of a gateway to the address you specify. If another gateway has a better route to the requested host, the default gateway sends an ICMP Redirect message back. The ICMP Redirect message indicates which local router the Cisco IOS software should use.

Examples

The following example defines the router on IP address 192.168.7.18 as the default router:

```
DSLAM(config)# ip default-gateway 192.168.7.18
```

Related Commands

None.

ip dhcp conflict logging

To enable conflict logging on a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server, use the **ip dhcp conflict logging** global configuration command. Use the **no** form of this command to disable conflict logging.

ip dhcp conflict logging

no ip dhcp conflict logging

Syntax Description

This command has no arguments or keywords.

Defaults

Conflict logging is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

We recommend that you use a DHCP server database agent to store automatic bindings. If you decide not to use a DHCP server database agent to store automatic bindings, use the **no ip dhcp conflict logging** command to disable the recording of address conflicts. By default, the Cisco IOS DHCP server records DHCP address conflicts in a log file.

Examples

The following example disables the recording of DHCP address conflicts:

```
DSLAM(config)# no ip dhcp conflict logging
```

Related Commands

Command	Description
clear ip dhcp conflict	Clears an address conflict from the Cisco IOS DHCP server database.
ip dhcp database	Configures a DHCP server database agent and database agent parameters.
show ip dhcp conflict	Displays address conflicts that a Cisco IOS DHCP server finds when addresses are offered to the client.

ip dhcp database

You can configure a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server to save automatic bindings on a remote host called a database agent. To configure a DHCP server database agent and database agent parameters, use the **ip dhcp database** global configuration command. Use the **no** form of this command to remove the database agent.

ip dhcp database *url* [**timeout** *seconds* | **write-delay** *seconds*]

no ip dhcp database *url*

Syntax Description

url	Specifies the remote file used to store the automatic bindings. The acceptable URL file formats include: • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename
timeout *seconds*	(Optional) Specifies how long, in seconds, the DHCP server should wait before ending a database transfer. Transfers that exceed the timeout period end. By default, DHCP waits 300 seconds before it ends a database transfer. Infinity is defined as 0 seconds.
write-delay *seconds*	(Optional) Specifies how soon the DHCP server should send database updates. By default, DHCP waits 300 seconds (5 minutes) before it sends database changes. The minimum delay is 60 seconds.

Defaults

DHCP waits 300 seconds for both a write delay and a timeout.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The administrator can configure multiple database agents. Transfer bindings by using the File Transfer Protocol (FTP), Trivial File Transport Protocol (TFTP), or Remote Copy Protocol (RCP).

Examples

The following example specifies the DHCP database transfer timeout value at 80 seconds:

```
DSLAM(config)# ip dhcp database ftp://user:password@172.16.1.1/router-dhcp timeout 80
```

The following example specifies the DHCP database update delay value at 100 seconds:

```
DSLAM(config)# ip dhcp database tftp://172.16.1.1/router-dhcp write-delay 100
```

Related Commands

Command	Description
show ip dhcp database	Displays Cisco IOS DHCP server database agent information.

ip dhcp excluded-address

To specify IP addresses that a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server should not assign to DHCP clients, use the **ip dhcp excluded-address** global configuration command. Use the **no** form of this command to remove the excluded IP addresses.

ip dhcp excluded-address *low-address* [*high-address*]

no ip dhcp excluded-address *low-address* [*high-address*]

Syntax Description

low-address	The excluded IP address, or first IP address in an excluded address range.
high-address	(Optional) The last IP address in the excluded address range.

Defaults

All IP pool addresses are assignable.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The DHCP server assumes that it can assign all pool addresses to clients. Use this command to exclude a single IP address or a range of IP addresses.

Examples

The following example configures an excluded IP address range from 172.16.1.100 through 172.16.1.199:

```
DSLAM(config)# ip dhcp excluded-address 172.16.1.100 172.16.1.199
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
network (DHCP)	Configures the subnet number and mask for a DHCP address pool on a Cisco IOS DHCP server.

ip dhcp ping packets

To specify the number of packets that a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server sends to a pool address as part of a ping operation, use the **ip dhcp ping packets** global configuration command. Use the **no** form of this command to prevent the server from pinging pool addresses.

ip dhcp ping packets *count*

no ip dhcp ping packets

Syntax Description

count	Indicates the number of ping packets that the DHCP server sends before the address is assigned to a requesting client. The default value is two packets.

Defaults

Two packets

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The DHCP server pings a pool address before it assigns the address to a requesting client. If the ping is unanswered, the DHCP server assumes (with a high degree of probability) that the address is not in use and assigns the address to the requesting client.

Examples

The following example specifies five ping attempts by the DHCP server before the server ceases any further ping attempts:

```
DSLAM(config)# ip dhcp ping packets 5
```

Related Commands

Command	Description
clear ip dhcp conflicts	Clears an address conflict from the Cisco IOS DHCP server database.
ip dhcp ping timeout	Specifies how long a Cisco IOS DHCP server waits for a ping reply from an address pool.
show ip dhcp conflict	Displays address conflicts that a Cisco IOS DHCP server finds when addresses are offered to the client.

ip dhcp ping timeout

To specify how long a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server waits for a ping reply from an address pool, use the **ip dhcp ping timeout** global configuration command. Use the **no** form of this command to restore the default number of milliseconds (500) for the timeout.

ip dhcp ping timeout *milliseconds*

no ip dhcp ping timeout

Syntax Description

milliseconds	The amount of time in milliseconds that the DHCP server waits for a ping reply before it stops attempting to reach a pool address for client assignment. The maximum timeout is 10,000 milliseconds (10 seconds). The default timeout is 500 milliseconds.

Defaults

500 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

This command specifies how long to wait for a ping reply in milliseconds.

Examples

The following example specifies that the DHCP server will wait 800 milliseconds for a ping reply before considering the ping a failure:

```
DSLAM(config)# ip dhcp ping timeout 800
```

Related Commands

Command	Description
clear ip dhcp conflicts	Clears an address conflict from the Cisco IOS DHCP server database.
ip dhcp ping packets	Specifies the number of packets that a Cisco IOS DHCP server sends to a pool address as part of a ping operation.
show ip dhcp conflict	Displays address conflicts that a Cisco IOS DHCP server finds when addresses are offered to the client.

ip dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) address pool on a Cisco IOS DHCP server and enter DHCP pool configuration mode, use the **ip dhcp pool** global configuration command. Use the **no** form of this command to remove the address pool.

ip dhcp pool *name*

no ip dhcp pool *name*

Syntax Description

name	Can be either a symbolic string (such as “engineering”) or an integer (such as 0).

Defaults

DHCP address pools are not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

During execution, the configuration mode changes to DHCP pool configuration mode, which is identified by the (config-dhcp)# prompt. In this mode, the administrator can configure pool parameters, such as the IP subnet number and default router list.

Examples

The following example configures pool1 as the DHCP address pool:

```
DSLAM(config)# ip dhcp pool pool1
```

Related Commands

This command is used by cable modem termination systems. By default, DHCP checks relay information. Invalid messages are dropped.

ip dhcp relay information option

To configure a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages, use the **ip dhcp relay information option** global configuration command. Use the **no** form of this command to disable the insertion of relay information to forwarded BOOTREQUEST messages.

ip dhcp relay information option

no ip dhcp relay information option

Syntax Description

This command has no arguments or keywords.

Defaults

The DHCP server does not insert relay information.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

This command is used by cable modem termination systems. By default, DHCP does not insert relay information.

Examples

The following example configures a DHCP server to insert the DHCP relay agent information option in forwarded BOOTREQUEST messages:

```
DSLAM(config)# ip dhcp relay information option
```

Related Commands

Command	Description
ip dhcp relay information check	Configures a Cisco IOS DHCP server to validate the relay agent information option in forwarded BOOTREPLY messages.
ip dhcp relay information policy	Configures DHCP relay agent information reforwarding policy (what a DHCP relay agent should do if a message already contains relay information).

ip helper-address

To have the Cisco IOS software forward User Datagram Protocol (UDP) broadcasts, including BOOTP, that are received on an interface, use the **ip helper-address** interface configuration command. To disable the forwarding of broadcast packets to specific addresses, use the **no** form of this command.

ip helper-address *address*

no ip helper-address *address*

Syntax Description

address	Destination broadcast or host address to be used when forwarding UDP broadcasts. There can be more than one helper address per interface.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

One common application that requires helper addresses is Dynamic Host Configuration Protocol (DHCP), which is defined in RFC 1531. DHCP protocol information is carried inside of BOOTP packets. To enable BOOTP broadcast forwarding for a set of clients, configure a helper address on the router interface that is closest to the client. The helper address should specify the address of the DHCP server. If you have multiple servers, you can configure one helper address for each server. Because BOOTP packets are forwarded by default, DHCP information can now be forwarded by the router. The DHCP server then receives broadcasts from the DHCP clients.

Note The **ip helper-address** command does not work on an X.25 interface on a destination router because the router is unable to determine whether the packet was intended as a physical broadcast.

Examples

In the following example, DHCP option 82 support is enabled on the DHCP relay agent using the **ip dhcp relay agent information option** command. The **rbe nasip** command configures the DSLAM to forward the IP address for Loopback0 to the DHCP server.

```
DSLAM(config)# ip dhcp relay information option
DSLAM(config)# ip dhcp-server 10.0.0.202
DSLAM(config)# rbe nasip Loopback1
DSLAM(config)# interface Loopback1
DSLAM(config-if)# ip address 18.52.86.120 255.255.255.255
DSLAM(config-if)# interface Ethernet0/0
DSLAM(config-if)# ip address 10.0.0.40 255.0.0.0
DSLAM(config-if)# interface atm1/1
```

```
DSLAM(config-if)# ip address 11.0.0.1 255.0.0.0
DSLAM(config-if)# ip helper-address 10.0.0.202
DSLAM(config-if)# atm route-bridged ip
DSLAM(config-if)# no atm ilmi-keepalive
DSLAM(config-if)# pvc 1/1
DSLAM(config-if)# encapsulation aal5snap
DSLAM(config-if)# interface ATM1/2
DSLAM(config-if)# ip address 12.0.0.1 255.0.0.0
DSLAM(config-if)# ip helper-address 10.0.0.202
DSLAM(config-if)# atm route-bridged ip
DSLAM(config-if)# no atm ilmi-keepalive
DSLAM(config-if)# pvc 1/1
DSLAM(config-if)# encapsulation aal5snap
```

Related Commands None.

ip local pool

To configure a local IP address pool group, use the **ip local pool** configuration command with the group name. To disband the group, use the **no** form of this command.

ip local pool *pool-name start-IP* [*end-IP*] [**group** *group-name*] [**cache-size** *size*]

no ip local pool

Syntax Description

pool-name	User-defined name for the local address pool.
start-IP	IP address that defines the start of the group.
end-IP	IP address that defines the end of the contiguous addresses in the group.
group	Define a group that contains this pool.
group-name	User-defined name for the pool group.
cache-size	Specify the size of the cache.
size	Size of the cache.

Defaults

Any pool that you create without the optional **group** keyword is a member of the base system group.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

All pool names must be unique. Use of a duplicate name extends that pool.

If you specify a (named) pool within a pool group, the software allows overlapping IP addresses to exist with pools in other groups and with pools in the "base system" pool. The software does not allow the overlapping IP address to exist among pools within a group. Otherwise, pool processing is not altered by pool membership in a group. That is, you can use these (named) pools anywhere that pools can be used in the current implementation.

Addresses return to the pool from which they were allocated.

Examples

This example shows the configuration of two pool groups, including pools in the base system group.

```
DSLAM(config)# ip local pool p1_g1 10.1.1.1 10.1.1.50 group grp1
DSLAM(config)# ip local pool p2_g1 10.1.1.100 10.1.1.110 group grp1
DSLAM(config)# ip local pool p1_g2 10.1.1.1 10.1.1.40 group grp2
DSLAM(config)# ip local pool lp1 10.1.1.1 10.1.1.10
DSLAM(config)# ip local pool p3_g1 10.1.2.1 10.1.2.30 group grp1
DSLAM(config)# ip local pool p2_g2 10.1.1.50 10.1.1.70 group grp2
DSLAM(config)# ip local pool lp2 10.1.2.1 10.1.2.10
```

In this example, pool group “grp1” consists of pools “p1_g1,” “p2_g1,” and “p3_g1”; pool group “gp2” consists of pools “p1_g2” and “p2_g2”; and pools “lp1” and “lp2,” which are members of the base system group. Note the overlap addresses: IP address 1.1.1.1 is in all of them (“grp1” group, “grp2” group and the base system group). Also note that there is no overlap within any group (including the base system group, which is unnamed).

This example shows pool names that provide an easy way to associate a pool name with a group (when the pool name stands alone). While this can be an operational convenience, no relationship is required between the names used to define a pool and the name of the group.

Related Commands

Command	Description
debug ip peer	This command contains additional output when pool groups are defined.

ip route vrf

To establish static routes for a VRF, use the **ip route vrf** global configuration command. To disable static routes, use the **no** form of this command.

ip route vrf *vrf-name prefix mask* **{**[*next-hop-address*] | [*interface* {*interface-number*}]} **[global**] [*distance*] [**permanent**] [**tag** *tag*]

no ip route vrf *vrf-name prefix mask* **{**[*next-hop-address*] | [*interface* {*interface-number*}]} **[global**] [*distance*] [**permanent**] [**tag** *tag*]

Syntax Description

vrf-name	Name of the VPN routing or forwarding instance (VRF) for the static route.
prefix	IP route prefix for the destination, in dotted-decimal format.
mask	Prefix mask for the destination, in dotted-decimal format.
next-hop-address	(Optional) IP address of the next hop (the forwarding router that can be used to reach that network).
interface	(Optional) Type of network interface to use: ATM, Ethernet, loopback, POS (packet over SONET), or null.
interface-number	Number that identifies the network interface to use.
global	The given next hop address is in the nonVRF routing table.
distance	(Optional) An administrative distance for this route.
permanent	(Optional) This route will not be removed, even if the interface shuts down.
tag *tag*	(Optional) Label value that can be used for controlling redistribution of routes through route maps.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

Use a static route if the Cisco IOS software cannot dynamically build a route to the destination.

If you specify an administrative distance when you set up a route, you are flagging a static route that can be overridden by dynamic information. For example, IGRP-derived routes are configured with a default administrative distance of 100. To set a static route to be overridden by an IGRP dynamic route, specify an administrative distance greater than 100. Static routes each have a default administrative distance of 1.

Static routes that point to an interface are advertised through RIP, IGRP, and other dynamic routing protocols, regardless of whether the routes are redistributed into those routing protocols. That is, static routes configured by specifying an interface lose their static nature when installed into the routing table.

However, if you define a static route to an interface that is not defined in a network command, no dynamic routing protocols advertise the route unless you specify a redistribute static command for these protocols.

Examples

The following command shows how to reroute packets addressed to network 137.23.0.0 in VRF vpn3 to router 131.108.6.6:

```
DSLAM(config)# ip route vrf vpn3 137.23.0.0 255.255.0.0 131.108.6.6
```

Related Commands

Command	Description
show ip route vrf	Displays the IP routing table associated with a VRF.

ip routing

To enable IP routing, use the **ip routing** global configuration command. To disable IP routing, use the **no** form of this command.

ip routing

no ip routing

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Examples

The following example enables IP routing:

```
DSLAM(config)# ip routing
```

Related Commands

None.

ip subnet-zero

To enable the use of subnet zero for interface addresses and routing updates, use the **ip subnet-zero** global configuration command. To restore the default, use the **no** form of this command.

ip subnet-zero

no ip subnet-zero

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The **ip subnet-zero** command enables you to configure and route to subnet-zero subnets.

We discourage subnetting with a subnet address of zero because of the confusion inherent when you have a network and a subnet with indistinguishable addresses.

Examples

The following example enables subnet-zero:

```
DSLAM(config)# ip subnet-zero
```

Related Commands

None.

ip unnumbered

To enable IP processing on an ATM interface without assigning an explicit IP address to the interface, use the **ip unnumbered** interface configuration command. To disable the IP processing on the interface, use the **no** form of this command.

ip unnumbered *type number*

Syntax Description

type number	Type and number of another interface on which the router has an assigned IP address. This number cannot be another unnumbered interface.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

Whenever the unnumbered interface generates a packet (for example, for a routing update), it uses the address of the specified interface as the source address of the IP packet. The unnumbered interface also uses the address of the specified interface to determine which routing processes are sending updates over the unnumbered interface. Restrictions include the following:

- Serial interfaces using High-Level Data Link Control (HDLC), PPP, Link Access Procedure, Balanced (LAPB), and Frame Relay encapsulations, as well as Serial Line Internet Protocol (SLIP) and tunnel interfaces, can be unnumbered. You cannot use this interface configuration command with X.25 or Switched Multimegabit Data Service (SMDS) interfaces.
- You cannot use the **ping** EXEC command to determine whether the interface is up because the interface has no address. You can use Simple Network Management Protocol (SNMP) to remotely monitor interface status.
- You cannot netboot a runnable image over an unnumbered serial interface.
- You cannot support IP security options on an unnumbered interface.

The interface that you specify by the type and number arguments must be enabled (listed as "up" in the **show interfaces** command display).

If you are configuring IS-IS across a serial line, you should configure the serial interfaces as unnumbered. Doing so allows you to conform with RFC 1195, which states that IP addresses are not required on each interface.

Note The use of an unnumbered serial line between different major networks (majornets) requires special care. If at each end of the link different majornets are assigned to the interfaces that you specified as unnumbered, any routing protocol that is running across the serial line must not advertise subnet information.

Examples

In the following example, the first ATM interface is given the Ethernet 0/0 address:

```
DSLAM(config)# interface ethernet 0/0
DSLAM(config-if)# ip address 131.108.6.6 255.255.255.0
     !
DSLAM(config)# interface atm 0/1
DSLAM(config-if)# ip unnumbered ethernet 0/0
```

Related Commands

None.

ip vrf

To configure a VPN routing/forwarding (VRF) routing table, use the **ip vrf** global configuration command. To remove a VRF routing table, use the **no** form of this command.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Defaults

No VRFs are defined. No import or export lists are associated with a VRF. No route maps are associated with a VRF.

Command Modes

Router configuration

Global configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

The **ip vrf *vrf-name*** command creates a VRF routing table and a CEF (forwarding) table, both named *vrf-name*. The default route distinguisher value *route-distinguisher* is associated with these tables.

Examples

The following example shows how to import a route map to a VRF:

```
DSLAM(router-config)# ip vrf vpn1
DSLAM(config-vrf)# rd 100:2
DSLAM(config-vrf)# route-target both 100:2
DSLAM(config-vrf)# route-target import 100:1
```

Related Commands

Command	Description
ip vrf forwarding	Associates a VRF with an interface or subinterface.

ip vrf forwarding

To associate a VRF with an interface or subinterface, use the **ip vrf forwarding** interface configuration command. To disassociate a VRF, use the **no** form of this command.

ip vrf forwarding *vrf-name*

no ip vrf forwarding *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Defaults

The default for an interface is the global routing table.

Command Modes

Global configuration

Interface configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

Use this command to associate an interface with a VRF. Executing this command on an interface removes the IP address. You should reconfigure the IP address.

Examples

The following example shows how to link a VRF to ATM interface 1/1:

```
DSLAM(config)# interface atm1/1
DSLAM(config-if)# ip vrf forwarding vpn1
```

Related Commands

Command	Description
ip vrf	Defines a VRF.
ip route vrf	Establishes static routes for a VRF.

lbo

To set the line build-out to various lengths, use the **lbo** interface configuration command. To restore the default values, use the **no** form of this command.

lbo {*short {133 | 266 | 399 | 533 | 655}* | *long* {*gain10 | gain36*} {*0db | -7.5db | -15db | -22.5db*}}

no lbo

Syntax Description

short	Short cable length. Must be followed by a length value. The range mapping for each value is shown below:

Value	Range (feet)
133	0 to 133
266	134 to 266
399	267 to 399
533	400 to 533
655	534 to 655

long	Cable length line build out. The *long* setting must be followed by a gain and a margin value.

Defaults

The default setting is long haul with gain36 and 0 dB (**lbo long gain36 0db**).

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

This command is applicable to E1 and T1 links.

Examples

The following example shows how to select **long** as the cable length.

```
DSLAM(config)# interface atm 0/2
DSLAM(config-if)# lbo long gain36 -15db
```

The following example shows how to select **short** as the cable length.

```
DSLAM(config)# interface atm 0/2
DSLAM(config-if)# lbo short 266
```

Related Commands

Command	Description
show controllers	Displays information about a physical port device.

lease

To configure the duration of the lease for an IP address that is assigned from a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server to a DHCP client, use the **lease** DHCP pool configuration command. Use the **no** form of this command to restore the default value.

lease {*days* [*hours*][*minutes*] | **infinite**}

no lease

Syntax Description

days	Specifies the duration of the lease in number of days.
hours	(Optional) Specifies the number of hours in the lease. You must supply a *days* value before you can configure an *hours* value.
minutes	(Optional) Specifies the number of minutes in the lease. You must supply a *days* value and an *hours* value before you can configure a *minutes* value.
infinite	Specifies that the duration of the lease is unlimited.

Defaults

One day

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Examples

The following example shows a 1-day lease:

```
DSLAM# configure terminal
DSLAM(config)# ip dhcp pool test
DSLAM(dhcp-config)# lease 1
```

The following example shows a 1-hour lease:

```
DSLAM# configure terminal
DSLAM(config)# ip dhcp pool test
DSLAM(dhcp-config)# lease 0 1
```

The following example shows a 1-minute lease:

```
DSLAM# configure terminal
DSLAM(config)# ip dhcp pool test
DSLAM(dhcp-config)# lease 0 0 1
```

The following example shows an infinite (unlimited) lease:

```
DSLAM# configure terminal
DSLAM(config)# ip dhcp pool test
DSLAM(dhcp-config)# lease infinite
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

linecode

To select the line code type of the T1/E1 link, use the **linecode** interface configuration command. To restore the default values, use the **no** form of this command.

linecode {**ami | b8zs | hdb3**}

no linecode {**ami | b8zs | hdb3**}

Syntax Description

ami	Alternate mark inversion (AMI) as the line code type. Valid for T1 or E1 controllers.
b8zs	B8ZS as the line code type. Valid for T1 controller.
hdb3	HDB3 as the line code type. Valid for E1 controller.

Defaults

T1 = **b8zs**

E1 = **hdb3**

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

Use this command to match the line code of the far end device.

Examples

The following example specifies AMI as the line code type:

```
DSLAM(config)# interface atm 0/3
DSLAM(config-if)# linecode ami
```

Related Commands

Command	Description
show controllers	Displays information about a physical port device.

loopback

To enable a loopback on a port, use the **loopback** interface configuration command. To disable the loopback, use the **no** form of the command.

loopback {**diagnostic | line | payload**}

loopback [**diagnostic | line**] [**protection | working | <cr>**]

no loopback

Syntax Description

diagnostic	Transmit data is looped to receive data at the physical (PHY) layer. This option is available on all ports.
line	Configures the link to loop the received signal (T1/E1, E3, OC-3, or DS3) back out the transmitter with no changes in framing, coding, and so forth.
payload	Configures the link to remove the user data from the received T1/E1, E3, or DS3, reframes the user data, and transmits it out.
protection	The fiber that is connected to the NI-2 card in slot 11.
working	The fiber that is connected to the NI-2 card in slot 10.
<cr>	Both protection and working fibers.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.1(7)DA	The keywords **working** and **protection** were added.

Usage Guidelines

If you enable or disable loopbacks, the port does not untrain or retrain. However, if you remove a loopback, the port retrains. The **working** and **protection** keywords are available only when you are configuring loopback on a SONET port.

Examples

This command enables ATM local loopback for port 1 of slot 20, then disables the loopback:

```
DSLAM# configure terminal
DSLAM(config)# interface atm 20/1
DSLAM(config-if)# loopback diagnostic
DSLAM(config-if)# no loopback diagnostic
```

This command enables a line loopback for the trunk port:

```
DSLAM# configure terminal
DSLAM(config)# interface atm 0/1
DSLAM(config-if)# loopback line
```

The following example enables a loopback on atm 0/1, on the fiber local to the NI-2 card in slot 11:

```
DSLAM> enable
DSLAM# configure terminal
DSLAM(config)# interface atm 0/1
DSLAM(config-if)# loopback diagnostic protection
```

Related Commands

Command	Description
show controllers	Display information on working and protection fibers.

N Through shdsl Commands for Cisco DSLAMs with NI-2

This chapter documents commands that you use to configure Cisco DSLAMs with NI-2. Commands in this chapter are listed alphabetically. For information on how to configure DSL features, refer to the *Configuration Guide for Cisco DSLAMs with NI-2*.

Note Commands that are identical to those documented in the *Cisco IOS Configuration Fundamentals Command Reference* and the *ATM and Layer 3 Switch Router Command Reference* have been removed from this chapter.

This chapter discusses the following commands:

neighbor activate

network (DHCP)

option

payload-scrambling

peer default ip address

ppp authentication

ppp chap hostname

protocol

radius-server attribute nas-port format

radius-server challenge-noecho

radius-server configure-nas

radius-server deadtime

radius-server directed-request

radius-server host

radius-server host non-standard

radius-server key

radius-server optional passwords

radius-server retransmit

radius-server timeout

radius-server vsa send

rbe nasip

rd

redundancy reload-peer

redundancy reload-shelf

redundancy switch-activity

request-dialin

route-target

scrambling

sdsl bitrate

secondary sync bootflash

secondary sync config

secondary sync flash

secondary sync running-config

service dhcp

set temperature-rating

shdsl annex

shdsl bitrate

shdsl margin

shdsl masktype

shdsl ratemode

shdsl set bitrate masktype annex

neighbor activate

To enable the exchange of information with a BGP neighboring router, use the **neighbor activate** router configuration command. To disable the exchange of an address with a neighboring router, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **activate**

no neighbor {*ip-address* | *peer-group-name*} **activate**

Syntax Description

ip-address	IP address of the neighboring router.
peer-group-name	Name of BGP peer group.

Defaults

The exchange of addresses with neighbors is enabled by default for the VPN IPv4 address family. You can disable IPv4 address exchange using the general command **no default bgp ipv4 activate**, or you can disable it for a particular neighbor using the **no** form of this command.

For all other address families, address exchange is disabled by default. You can explicitly activate the default command using the appropriate address family submode.

Command Modes

Router configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

Use this command to enable or disable the exchange of addresses with a neighboring router.

Examples

In the following example, a BGP router activates the exchange of a customer's IP address 10.15.0.15 to a neighboring router:

```
DSLAM(config)# router bgp 100
DSLAM(config-router)# neighbor 10.15.0.15 remote-as 100
DSLAM(config-router)# neighbor 10.15.0.15 update-source loopback0
DSLAM(config-router)# address-family vpnv4 unicast
DSLAM(config-router-af)# neighbor 10.15.0.15 activate
DSLAM(config-router-af)# exit-address-family
```

Related Commands

Command	Description
address-family	Enters the address-family submode.
exit-address-family	Exits the address-family submode.

network (DHCP)

To configure the subnet number and mask for a Dynamic Host Configuration Protocol (DHCP) address pool on a Cisco IOS DHCP server, use the **network** DHCP pool configuration command. Use the **no** form of this command to remove the subnet number and mask.

network *network-number* [*mask* | */prefix-length*]

no network

Syntax Description

network-number	The IP address of the DHCP address pool.
mask	(Optional) The bit combination that determines which portion of the address of the DHCP address pool refers to the network or subnet and which part refers to the host.
/prefix-length	(Optional) Specifies the number of bits that make up the address prefix. The prefix is an alternative way to specify the network mask of the client. Precede the prefix length by a forward slash (/).

Defaults

No default behavior or values.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

This command is valid only for DHCP subnetwork address pools. If you do not specify the mask or prefix length, the software uses the class A, B, or C natural mask. The DHCP server acts as if all host addresses are available. The system administrator can exclude subsets of the address space by using the **ip dhcp excluded-address** command.

Examples

The following example configures 172.16.0.0/16 as the DHCP pool subnetwork number and mask:

```
DSLAM# configure terminal
DSLAM(config)# ip dhcp pool 1
DSLAM(dhcp-config)# network 172.16.0.0 /16
```

Related Commands

Command	Description
host	Specifies the IP address and network mask for a manual binding to a DHCP client.
ip dhcp excluded-address	Specifies IP addresses that a Cisco IOS DHCP server should not assign to DHCP clients.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

option

To configure Cisco IOS Dynamic Host Configuration Protocol (DHCP) server options, use the **option** DHCP pool configuration command. Use the **no** form of this command to remove the options.

option *code* [**instance** *number*] {**ascii** *string* | **hex** *string* | **ip** *address*}

no option *code* [**instance** *number*]

Syntax Description

code	Specifies the DHCP option code.
instance *number*	(Optional) Specifies a number from 0 to 255.
ascii *string*	Specifies an NVT ASCII character string. Delineate ASCII character strings that contain white space by quotation marks.
hex *string*	Specifies dotted-hexadecimal data. Each byte in hexadecimal character strings is two hexadecimal digits—separate each byte with a period, colon, or white space.
ip *address*	Specifies an IP address.

Defaults

The default instance number is 0.

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

DHCP provides a framework for passing configuration information to hosts on a TCP/IP network. Configuration parameters and other control information are carried in tagged data items that you store in the options field of the DHCP message. The data items themselves are also called options. The current set of DHCP options is documented in RFC 2131, *Dynamic Host Configuration Protocol*.

Examples

The following example configures DHCP option 19, which specifies whether the client should configure its IP layer for packet forwarding. A value of 0 means disable IP forwarding; a value of 1 means enable IP forwarding. IP forwarding is enabled in the following example:

```
DSLAM# configure terminal
DSLAM(config)# ip dhcp pool 1
DSLAM(dhcp-config)# option 19 hex 01
```

The following example configures DHCP option 72, which specifies the World Wide Web servers for DHCP clients. World Wide Web servers 172.16.3.252 and 172.16.3.253 are configured in the following example:

```
DSLAM# configure terminal
DSLAM(config)# ip dhcp pool 1
DSLAM(dhcp-config)# option 72 ip 172.16.3.252 172.16.3.253
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

payload-scrambling

To enable ATM cell payload scrambling on a DSL subscriber port, use the **payload-scrambling** profile configuration command. To disable payload scrambling, use the **no** form of the command.

payload-scrambling

no payload-scrambling

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

Profile configuration

Command History

Release	Modification
12.1(1)DA	This command was introduced.

Usage Guidelines

The two ends of a connection must have the same payload scrambling value—that is, payload scrambling must be enabled at both ends or disabled at both ends. The line trains if you enable payload scrambling at one end and disable it at the other end, but all AAL5 frames will have cyclic redundancy checks.

If you enable or disable payload scrambling, the port does not untrain or retrain.

Examples

This command disables payload scrambling for the default DSL profile:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile default
DSLAM(cfg-dsl-profile)# no payload-scrambling
```

Related Commands

Command	Description
show dsl profile	Displays a specific DSL profile.
show dsl interface atm *slot#/port#*	Displays the DSL and ATM status for a port.

peer default ip address

Use the **peer default ip address** command to specify an IP address, an address from a specific IP address pool, or an address from the DHCP mechanism that is to be returned to a remote peer connecting to this interface. Use the **no** form of the command to disable a prior peer IP address pooling configuration on an interface.

peer default ip address {*ip-address* | **dhcp** | **pool** [*poolname*]}

no peer default ip address

Syntax Description

ip-address	Specific IP address to be assigned to a remote peer that dials in to the interface. To prevent an IP addresse from being assigned on more than one interface, you cannot apply this command argument to a dialer rotary group or to an ISDN interface.
dhcp	Retrieve an IP address from the DHCP server.
pool	Use the Global Default Mechanism as defined by the **ip address-pool** command unless the optional *poolname* argument is supplied.
poolname	(Optional) Name of a local address pool created using the **ip local pool** command. Retrieve an address from this pool regardless of the Global Default Mechanism setting.

Defaults

pool

Command Modes

Interface configuration

Usage Guidelines

This command applies to point-to-point interfaces that support the PPP or SLIP encapsulation.

This command allows an administrator to configure all possible address pooling mechanisms on a interface-by-interface basis.

The **peer default ip address** command can override the Global Default Mechanism defined by the **ip address-pool** command on an interface-by-interface basis.

- For all interfaces that are not configured with a peer default IP address mechanism (equivalent to selecting the **peer default ip address pool** command), the router uses the Global Default Mechanism that is defined by the **ip address-pool** command.
- If you select the **peer default ip address pool** *poolname* form of this command, the router uses the locally configured pool on this interface and does not follow the Global Default Mechanism.
- If you select the **peer default ip address** *ip-address* form of this command, the specified IP address is assigned to any peer that connects to this interface and any Global Default Mechanism is overridden for this interface.
- If you select the **peer default ip address dhcp** form of this command, the software uses the DHCP proxy-client mechanism by default on this interface and overrides any Global Default Mechanism for this interface.

Examples

The following command specifies that this interface will use a local IP address pool called pool1:

```
DSLAM(config)# interface virtual-template 1
DSLAM(config-if)# peer default ip address pool pool1
```

The following command specifies that this interface will use the IP address 172.140.34.21:

```
DSLAM(config-if)# peer default ip address dhcp
```

The following command reenables the Global Default Mechanism that this interface will use:

```
DSLAM(config-if)# peer default ip address pool
```

Related Commands

Command	Description
encapsulation	Sets the encapsulation method used by the interface.
ppp authentication	Enables Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) and enables an AAA authentication method on an interface.

ppp authentication

To enable Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) and to enable an AAA authentication method on an interface, use the **ppp authentication** interface configuration command. Use the **no** form of this command to disable this authentication.

ppp authentication {chap | pap} [if-needed] [list-name]

no ppp authentication

Caution If you use a list-name value that was not configured with the aaa authentication ppp command, you disable PPP on this interface.

Syntax Description

chap	Enables CHAP on a serial interface.
pap	Enables PAP on a serial interface.
if-needed	(Optional) Used with TACACS and extended TACACS. Does not perform CHAP or PAP authentication if the user has already provided authentication. This option is available only on asynchronous interfaces.
list-name	(Optional) Used with AAA. Specifies the name of a list of AAA methods of authentication to use. If you do not specify a listname, the system uses the default. You create lists and defaults with the **aaa authentication ppp** command.

Defaults

PPP authentication is not enabled.

Command Modes

Interface configuration

Command History

Command	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

When you enable CHAP or PAP, the local router requires a password from remote devices. If the remote device does not support CHAP or PAP, no traffic is passed to that device.

If you use autoselect on a TTY line, you will probably want to use the **ppp authentication** command to turn on PPP authentication for the corresponding interface.

If you specify the if-needed option, the software does not require PPP authentication when you have already provided authentication. This option is useful if you specify the **autoselect** command, but you cannot use it with AAA.

You can use the list-name argument only when AAA is initialized; you cannot use it with the if-needed argument.

Examples

The following example enables CHAP on asynchronous interface 1, and uses the authentication list MIS-access:

```
DSLAM(config)# interface async 1
DSLAM(config-if)# encapsulation ppp
DSLAM(config-if)# ppp authentication chap MIS-access
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa new-model	Enables the AAA access control model.
encapsulation ppp	Sets the encapsulation method that the interface uses.

ppp chap hostname

To create a pool of dialup routers that all appear to be the same host when you are authenticating with CHAP, use the **ppp chap hostname** interface configuration command. To disable this function, use the **no** form of the command.

ppp chap hostname *hostname*

no ppp chap hostname *hostname*

Syntax Description

hostname	The name sent in the CHAP challenge.

Defaults

Disabled. The router name is sent in any CHAP challenges.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

Currently, a router that dials a pool of access routers requires a username entry for each possible router in the pool because each router challenges with its hostname. If you add a router to the dialup rotary pool, you must update all connecting routers. The **ppp chap hostname** command allows you to specify a common alias for all routers in a rotary group so that you must configure only one username on the dialing routers.

You normally use this command with local CHAP authentication (when the router authenticates to the peer), but you can also use it for remote CHAP authentication.

Examples

The commands in the following example identify dialer interface 0 as the dialer rotary group leader and specify PPP as the encapsulation method that all member interfaces use. This example uses CHAP authentication on received calls only and sends the username *ISPCorp* in all CHAP challenges and responses:

```
DSLAM(config-if)# interface dialer 0
DSLAM(config-if)# encapsulation ppp
DSLAM(config-if)# ppp authentication chap callin
DSLAM(config-if)# ppp chap hostname ISPCorp
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on ATM and DSL interfaces running PPP.
ppp authentication	Enables Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) and enables an AAA authentication method on an interface.

protocol

To specify the tunneling protocol the dial-in connection uses, use the **protocol** accept-dialin VPDN group configuration command. Use the **no** form of this command to remove the options.

protocol {**any | l2f | l2tp | pppoe | pptp**}

Syntax Description

any	Use any protocol.
l2f	Use L2F.
l2tp	Use L2TP.
pppoe	Use PPPoE.
pptp	Use PPTP.

Defaults

If you use this command under the VPDN-group, the default protocol is **l2f**. Otherwise, there is no default.

Command Modes

accept-dialin VPDN group configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Examples

The following example requests an L2TP dial-in tunnel to a local host named lac1 at IP address 123.45.67.891 for a user in the domain named partner.com:

```
DSLAM(config)# vpdn enable
DSLAM(config)# vpdn-group l2tp-group
DSLAM(config-vpdn)# protocol l2tp
DSLAM(config-vpdn)# domain partner.com
DSLAM(config-vpdn)# initiate-to ip 123.45.67.891
DSLAM(config-vpdn)# local name lac1
DSLAM(config-vpdn)# source-ip 123.45.67.891
```

Related Commands

None.

radius-server attribute nas-port format

To select the NAS-Port format used for RADIUS accounting features, use the **radius-server attribute nas-port format** global configuration command. To restore the default NAS-Port format, use the **no** form of this command.

radius-server attribute nas-port format *format*

no radius-server attribute nas-port format *format*

Syntax Description

format	NAS-Port format. Possible values for the format argument are as follows: **a**—Standard NAS-Port format **b**—Extended NAS-Port format **c**—Shelf-slot NAS-Port format **d**—PPP extended NAS-Port format **e**—DSLAM extended NAS-Port format

Defaults

Standard NAS-Port format

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The **radius-server attribute nas-port format** command configures RADIUS to change the size and format of the NAS-Port attribute field (RADIUS IETF attribute 5).

The following NAS-Port formats are supported:

- Standard NAS-Port format—This 16-bit NAS-Port format indicates the type, port, and channel of the controlling interface. This is the default format used by Cisco IOS software.
- Extended NAS-Port format—The standard NAS-Port attribute field is expanded to 32 bits. The upper 16 bits of the NAS-Port attribute display the type and number of the controlling interface; the lower 16 bits indicate the interface that is undergoing authentication.
- Shelf-slot NAS-Port format—This 16-bit NAS-Port format supports expanded hardware models that require shelf and slot entries.
- PPP extended NAS-Port format—This NAS-Port format uses 32 bits to indicate the interface, VPI, and VCI for PPP over ATM and PPPoE over ATM, and the interface and VLAN ID for PPPoE over IEEE 802.1Q VLANs.

In the following example, a RADIUS server is identified, and the NAS-Port field is set to the PPP extended format:

```
DSLAM(config)# aaa new-model
DSLAM(config)# radius-server host 172.31.5.96 auth-port 1645 acct-port 1646
DSLAM(config)# radius-server attribute nas-port format d
```

Related Commands None.

radius-server challenge-noecho

To prevent the display of user responses to Access-Challenge packets, use the **radius-server challenge-noecho** global configuration command. To return to the default condition, use the **no** form of this command.

radius-server challenge-noecho

no radius-server challenge-noecho

Syntax Description

This command has no arguments or keywords.

Defaults

All user responses to Access-Challenge packets are echoed to the screen.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

This command applies to all users. When you configure the **radius-server challenge-noecho** command, user responses to Access-Challenge packets do not display unless the Prompt attribute in the user profile is set to *echo* on the RADIUS server. The Prompt attribute in a user profile overrides the **radius-server challenge-noecho** command for the individual user. For more information, see the chapter "Configuring RADIUS" in the *Cisco IOS Security Configuration Guide*, Release 12.2.

Examples

The command in the following example stops all user responses from displaying on the screen:

```
DSLAM(config)# aaa new-model
DSLAM(config)# radius-server challenge-noecho
```

Related Commands

None.

radius-server configure-nas

To have the Cisco router or access server query the vendor-proprietary RADIUS server for the static routes and IP pool definitions used throughout its domain when the device starts up, use the **radius-server configure-nas** command in global configuration mode. To discontinue the query of the RADIUS server, use the **no** form of this command.

radius-server configure-nas

no radius-server configure-nas

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

Use the **radius-server configure-nas** command to have the Cisco router query the vendor-proprietary RADIUS server for static routes and IP pool definitions when the router first starts up. Some vendor-proprietary implementations of RADIUS let the user define static routes and IP pool definitions on the RADIUS server instead of on each individual network access server in the network. As each network access server starts up, it queries the RADIUS server for static route and IP pool information. This command enables the Cisco router to obtain static routes and IP pool definition information from the RADIUS server.

Note Because the **radius-server configure-nas** command is performed when the Cisco router starts up, it does not take effect until you issue the **copy system:running-config nvram:startup-config** command.

Examples

The following example shows how to tell the Cisco router or access server to query the vendor-proprietary RADIUS server for already-defined static routes and IP pool definitions when the device first starts up:

```
DSLAM(config)# aaa new-model
DSLAM(config)# radius-server configure-nas
```

Related Commands

Command	Description
radius-server host non-standard	Indicates that the security server is using a vendor-proprietary implementation of RADIUS.

radius-server deadtime

To improve RADIUS response times when some servers might be unavailable, use the **radius-server deadtime** command in global configuration mode to cause the unavailable servers to be skipped immediately. To set dead time to 0, use the **no** form of this command.

radius-server deadtime *minutes*

no radius-server deadtime

Syntax Description

minutes	Length of time, in minutes, for which transaction requests skip over a RADIUS server, up to a maximum of 1440 minutes (24 hours).

Defaults

Dead time is set to 0.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

Use this command to cause the Cisco IOS software to mark as "dead" any RADIUS servers that fail to respond to authentication requests. This enables you to avoid the wait for the request to time out before the next configured server is tried. A RADIUS server marked as "dead" is skipped by additional requests for the duration of *minutes* or unless all servers are marked "dead."

Examples

The following example specifies 5 minutes dead time for RADIUS servers that fail to respond to authentication requests:

```
DSLAM(config)# aaa new-model
DSLAM(config)# radius-server deadtime 5
```

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server retransmit	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval for which a router waits for a server host to reply.

radius-server directed-request

To allow users who are logging into a Cisco network access server (NAS) to select a RADIUS server for authentication, use the **radius-server directed-request** global configuration command. To disable the directed-request feature, use the **no** form of this command.

radius-server directed-request [**restricted**]

no radius-server directed-request [**restricted**]

Syntax Description

restricted	(Optional) Prevents the user from being sent to a secondary server if the specified server is unavailable.

Defaults

User cannot log into a Cisco NAS to select a RADIUS server for authentication.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The **radius-server directed-request** command sends only the portion of the username before the "@" symbol to the host specified after the "@" symbol. In other words, with this command enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

If you disable the **radius-server directed-request** command, the whole string, both before and after the "@" symbol, is sent to the default RADIUS server. The router queries the list of servers, starting with the first one in the list. The router sends the whole string and accepts the first response that it gets from the server.

Use the **radius-server directed-request restricted** command to limit the user to the RADIUS server that is identified as part of the username.

The **no radius-server directed-request** command causes the entire username string to be passed to the default RADIUS server.

Examples

The following example verifies that the RADIUS server is selected based on the directed request:

```
DSLAM(config)# aaa new-model
DSLAM(config)# aaa authentication login default radius
DSLAM(config)# radius-server host 192.168.1.1
DSLAM(config)# radius-server host 172.16.56.103
DSLAM(config)# radius-server host 172.31.40.1
DSLAM(config)# radius-server directed-request
```

Related Commands

None.

radius-server host

To specify a RADIUS server host, use the **radius-server host** command in global configuration mode. To delete the specified RADIUS host, use the **no** form of this command.

radius-server host {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*] [**alias**{*hostname* | *ip-address*}]

no radius-server host {*hostname* | *ip-address*}

Syntax Description

hostname	Domain Name System (DNS) name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.
auth-port	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests.
port-number	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1645.
acct-port	(Optional) Specifies the UDP destination port for accounting requests.
port-number	(Optional) Port number for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 1646.
timeout	(Optional) The time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the **radius-server timeout** command. If no timeout value is specified, the global value is used. Enter a value in the range 1 to 1000.
seconds	(Optional) Specifies the **timeout** value. Enter a value in the range 1 to 1000. If you do not specify a **timeout** value, the global value is used.
retransmit	(Optional) The number of times a RADIUS request is re-sent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the **radius-server retransmit** command.
retries	(Optional) Specifies the retransmit value. Enter a value in the range 1 to 100. If you do not specify a retransmit value, the global value is used.
key	(Optional) Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This key overrides the global setting of the **radius-server key** command. If you do not specify a key string, the global value is used. The key is a text string that must match the encryption key that the RADIUS server uses. Always configure the key as the last item in the **radius-server host** command syntax. This syntax is necessary because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
string	(Optional) Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
alias	(Optional) Allows up to eight aliases per line for any given RADIUS server.

Defaults No RADIUS host is specified; use global **radius-server** command values.

Command Modes Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines You can use multiple **radius-server host** commands to specify multiple hosts. The software searches for hosts in the order in which you specify them.

If no host-specific timeout, retransmit, or key values are specified, the global values apply to each host.

Examples The following example specifies *host1* as the RADIUS server and uses default ports for both accounting and authentication:

```
DSLAM(config)# aaa new-model
DSLAM(config)# radius-server host host1
```

The following example specifies port 1612 as the destination port for authentication requests and port 1616 as the destination port for accounting requests on the RADIUS host named host1:

```
DSLAM(config)# aaa new-model
DSLAM(config)# radius-server host host1 auth-port 1612 acct-port 1616
```

Because entering a line resets all the port numbers, you must specify a host and configure accounting and authentication ports on a single line.

The following example specifies the host with IP address 172.29.39.46 as the RADIUS server, uses ports 1612 and 1616 as the authorization and accounting ports, sets the timeout value to 6, sets the retransmit value to 5, and sets “rad123” as the encryption key, matching the key on the RADIUS server:

```
DSLAM(config)# aaa new-model
DSLAM(config)# radius-server host 172.29.39.46 auth-port 1612 acct-port 1616 timeout 6
DSLAM(config)# retransmit 5 key rad123
```

To use separate servers for accounting and authentication, use the zero port value as appropriate.

The following example specifies that RADIUS server host1 be used for accounting but not for authentication, and that RADIUS server host2 be used for authentication but not for accounting:

```
DSLAM(config)# aaa new-model
DSLAM(config)# radius-server host host1.example.com auth-port 0
DSLAM(config)# radius-server host host2.example.com acct-port 0
```

The following example specifies four aliases on the RADIUS server with IP address 172.1.1.1:

```
DSLAM(config)# aaa new-model
DSLAM(config)# radius-server host 172.1.1.1 acct-port 1645 auth-port 1646
DSLAM(config)# radius-server host 172.1.1.1 alias 172.16.2.1 172.17.3.1 172.16.4.1
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to a user.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentications are selected on the interface.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit	Specifies how many times the Cisco IOS software searches the list of RADIUS server hosts before it gives up.
radius-server timeout	Sets the interval that a router waits for a server host to reply.

radius-server host non-standard

To identify that the security server is using a vendor-proprietary implementation of RADIUS, use the **radius-server host non-standard** command in global configuration mode. This command tells the Cisco IOS software to support nonstandard RADIUS attributes. To delete the specified vendor-proprietary RADIUS host, use the **no** form of this command.

radius-server host {*hostname* | *ip-address*} **non-standard**

no radius-server host {*hostname* | *ip-address*} **non-standard**

Syntax Description

hostname	DNS name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.

Defaults

No RADIUS host is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The **radius-server host non-standard** command enables you to indicate that the RADIUS server is using a vendor-proprietary implementation of RADIUS. Although an IETF draft standard for RADIUS specifies a method for communicating information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. This command enables the Cisco IOS software to support the most common vendor-proprietary RADIUS attributes. Vendor-proprietary attributes are not supported unless you use the **radius-server host non-standard** command.

For a list of supported vendor-specific RADIUS attributes, refer to the appendix "RADIUS Attributes" in the *Cisco IOS Security Configuration Guide*.

Examples

The following example specifies a vendor-proprietary RADIUS server host named *alcatraz*:

```
DSLAM(config)# aaa new-model
DSLAM(config)# radius-server host alcatraz non-standard
```

Related Commands

Command	Description
radius-server configure-nas	Allows the Cisco router or access server to query the vendor-proprietary RADIUS server for the static routes and IP pool definitions it uses throughout its domain when the device starts up.
radius-server host	Specifies a RADIUS server host.

radius-server key

To set the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon, use the **radius-server key** command in global configuration mode. To disable the key, use the **no** form of this command.

radius-server key {**0** *string* | **7** *string* | *string*}

no radius-server key

Syntax Description

0	Specifies that an unencrypted key will follow.
string	The unencrypted (cleartext) shared key.
7	Specifies that a hidden key will follow.
string	The hidden shared key.
string	The unencrypted (cleartext) shared key.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

After enabling authentication, authorization, and accounting (AAA) authentication with the **aaa new-model** command, you must set the authentication and encryption key using the **radius-server key** command.

Note Specify a RADIUS key after you issue the **aaa new-model** command.

The key that you enter must match the key that the RADIUS daemon uses. The software ignores all leading spaces, but it uses spaces within and at the end of the key. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

Examples

The following example sets the authentication and encryption key to “dare to go”:

```
DSLAM(config)# aaa new-model
DSLAM(config)# radius-server key dare to go
```

The following example sets the authentication and encryption key to “anykey.” The 7 specifies that a hidden key will follow.

```
DSLAM(config)# aaa new-model
DSLAM(config)# service password-encryption
DSLAM(config)# radius-server key 7 anykey
```

After you save your configuration and use the **show-running config** command, an encrypted key displays as follows:

```
DSLAM> show running-config
!
!
radius-server key 7 19283103834782sda
!The leading 7 indicates that the following text is encrypted.
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
ppp authentication	Enables CHAP or PAP or both and specifies the authentication method for CHAP and PAP authentication on the interface.
radius-server host	Specifies a RADIUS server host.

radius-server optional passwords

To specify that the first RADIUS request to a RADIUS server be made *without* password verification, use the **radius-server optional-passwords** command in global configuration mode. To restore the default, use the **no** form of this command.

radius-server optional-passwords

no radius-server optional-passwords

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

When the user enters the login name, the login request transmits with the name and a zero-length password. If accepted, the login procedure completes. If the RADIUS server refuses this request, the server software prompts for a password and tries again when the user supplies a password. The RADIUS server must support authentication for users without passwords to make use of this feature.

Examples

The following example configures the first login so that it does not require RADIUS verification:

```
DSLAM(config)# aaa new-model
DSLAM(config)# radius-server optional-passwords
```

Related Commands

None.

radius-server retransmit

To specify the number of times the Cisco IOS software searches the list of RADIUS server hosts before it gives up, use the **radius-server retransmit** command in global configuration mode. To disable retransmission, use the **no** form of this command.

radius-server retransmit *retries*

no radius-server retransmit

Syntax Description

retries	Maximum number of retransmission attempts. The default is 3 attempts.

Defaults

3 attempts

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The Cisco IOS software tries all servers, allowing each one to time out before it increases the retransmit count.

Examples

The following example specifies a retransmit counter value of five times:

```
DSLAM(config)# aaa new-model
DSLAM(config)# radius-server retransmit 5
```

Related Commands

None.

radius-server timeout

To set the interval for which a router waits for a server host to reply, use the **radius-server timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

radius-server timeout *seconds*

no radius-server timeout

Syntax Description

seconds	Number that specifies the timeout interval, in seconds. The default is 5 seconds.

Defaults

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

Use this command to set the number of seconds a router waits for a server host to reply before timing out.

Examples

The following example changes the interval timer to 10 seconds:

```
DSLAM(config)# aaa new-model
DSLAM(config)# radius-server timeout 10
```

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

radius-server vsa send

To configure the network access server to recognize and use vendor-specific attributes, use the **radius-server vsa send** command in global configuration mode. To restore the default, use the **no** form of this command.

radius-server vsa send [**accounting** | **authentication**]

no radius-server vsa send [**accounting** | **authentication**]

Syntax Description

accounting	(Optional) Limits the set of recognized vendor-specific attributes to only accounting attributes.
authentication	(Optional) Limits the set of recognized vendor-specific attributes to only authentication attributes.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the network access server and the RADIUS server by using the vendor-specific attribute (attribute 26). Vendor-specific attributes (VSAs) allow vendors to support their own extended attributes that are unsuitable for general use. The **radius-server vsa send** command enables the network access server to recognize and use both accounting and authentication vendor-specific attributes. Use the **accounting** keyword with the **radius-server vsa send** command to limit the set of recognized vendor-specific attributes to only accounting attributes. Use the **authentication** keyword with the **radius-server vsa send** command to limit the set of recognized vendor-specific attributes to only authentication attributes.

The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor-ID is 9, and the supported option has vendor-type 1, which is named “cisco-avpair.” The value is a string with the following format:

```
protocol : attribute sep value *
```

“Protocol” is a value of the Cisco “protocol” attribute for a particular type of authorization. “Attribute” and “value” are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and “sep” is “=” for mandatory attributes and “*” for optional attributes. This syntax allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes the Cisco "multiple named ip address pools" feature to be activated during IP authorization (during the PPP IPCP address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

The following example causes a "NAS Prompt" user to have immediate access to EXEC commands:

```
cisco-avpair= "shell:priv-lvl=15"
```

Other vendors have their own unique vendor-IDs, options, and associated VSAs. For more information about vendor-IDs and VSAs, refer to RFC 2138, *Remote Authentication Dial-In User Service (RADIUS)*.

Examples

The following example configures the network access server to recognize and use vendor-specific accounting attributes:

```
DSLAM(config)# aaa new-model
DSLAM(config)# radius-server vsa send accounting
```

Related Commands

Command	Description
radius-server attribute nas-port format	Selects the NAS-Port format used for RADIUS accounting features.

rbe nasip

To configure DHCP relay agent information option (option 82) support for ATM routed bridge encapsulation (RBE), use the **rbe nasip** command in global configuration mode. To remove this specification, use the **no** form of this command.

rbe nasip *source_interface*

no rbe nasip *source_interface*

Syntax Description

source_interface	The type and number of one of the interfaces on the router. The system forwards the IP address for this interface in the agent remote ID suboption, and the DHCP server uses the IP address to uniquely identify the DHCP relay agent.

Defaults

No IP address is specified.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

Use the **rbe nasip** command to configure DHCP relay agent information option (option 82) support for ATM routed bridge encapsulation (RBE).

You must configure DHCP relay agent information option support on the DHCP relay agent through the use of the **ip dhcp relay information option** command in order for the **rbe nasip** command to be effective.

Examples

In the following example, DHCP option 82 support is enabled on the DHCP relay agent with the **ip dhcp relay agent information option** command. The **rbe nasip** command configures the router to forward the IP address for Loopback0 to the DHCP server. ATM routed bridge encapsulation is configured on ATM subinterface 4/0.1.

```
DSLAM(config)# ip dhcp-server 10.0.0.202
!
DSLAM(config)# ip dhcp relay agent information option
!
DSLAM(config)# interface Loopback0
DSLAM(config-if)# ip address 18.52.86.120 255.255.255.255
!
DSLAM(config-if)# interface ATM4/0
DSLAM(config-if)# no ip address
!
DSLAM(config-if)# interface ATM4/0.1 point-to-point
DSLAM(config-if)# ip unnumbered Loopback0
```

```
DSLAM(config-if)# ip helper-address 170.16.1.2
DSLAM(config-if)# atm route-bridged ip
DSLAM(config-if)# pvc 88/800
DSLAM(config-if)# encapsulation aal5snap
!
DSLAM(config-if)# router eigrp 100
DSLAM(config-if)# network 11.0.0.0
DSLAM(config-if)# network 170.16.0.0
!
DSLAM(config-if)# rbe nasip loopback0
```

Related Commands

Command	Description
ip dhcp relay information option	Enables the system to insert the DHCP relay agent information option in forwarded BOOT REQUEST messages to a Cisco IOS DHCP server.

rd

To create routing and forwarding tables for a VRF, use the **rd** VRF submode command.

rd *route-distinguisher*

Syntax Description

route-distinguisher	Add an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix.

Defaults

There is no default. You must configure a route distinguisher for a VRF to be functional.

Command Modes

VRF submode

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

A route-distinguisher creates routing and forwarding tables and specifies the default route-distinguisher for a VPN. The software adds the route distinguisher to the beginning of the IPv4 prefixes to make the VPN-IPv4 prefixes globally unique.

A route distinguisher is either ASN-relative, in which case it is composed of an autonomous system number and an arbitrary number, or it is IP-address-relative, in which case it is composed of an IP address and an arbitrary number.

You can enter a route distinguisher in either of these formats:

16-bit AS number: your 32-bit number
For example, 101:3

32-bit IP address: your 16-bit number
For example, 192.168.122.15:1

Examples

The following example shows how to configure a default route distinguisher for two VRFs. The example illustrates the use of both AS-relative and IP address-relative route distinguishers:

```
DSLAM(config)# ip vrf vrf_blue
DSLAM(config-vrf)# rd 100:3
DSLAM(config-vrf)# ip vrf vrf_red
DSLAM(config-vrf)# rd 173.13.0.12:200
```

Related Commands

Command	Description
ip vrf	Enters VRF configuration mode.
show ip vrf	Displays information about a VRF.

redundancy reload-peer

To reload the standby NI-2 card, use the **redundancy reload-peer** privileged EXEC command.

redundancy reload-peer

Syntax Description

This command has no argument or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Usage Guidelines

This command reloads the standby NI-2 card in slot 11.

Examples

The following example reloads the standby NI-2 card:

```
DSLAM> enable
DSLAM# redundancy reload-peer
```

Related Commands

Command	Description
redundancy reload-shelf	Reload all cards in the chassis.
redundancy switch-activity	Switch over manually from the active NI-2 card to the standby NI-2 card.
show redundancy states	Display the state of the primary and secondary NI-2s, and identify which NI-2 is active.

redundancy reload-shelf

To reload all cards in the chassis, including the NI-2 cards, use the **redundancy reload-shelf** privileged EXEC command.

redundancy reload-shelf

Syntax Description

This command has no argument or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Usage Guidelines

This command reloads all the cards in the chassis. This command also prompts you for confirmation to save the running configuration if it has changed. If you enter "yes," the system saves the running configuration and then reloads all the cards in the chassis. If you enter "no," the system directly reloads all the cards in the chassis.

Examples

The command in the following example reloads all cards in the chassis:

```
DSLAM> enable
DSLAM# redundancy reload-shelf
System configuration has been modified. Save? [yes/no]: no
Reload the entire shelf [confirm] y
```

Related Commands

Command	Description
redundancy reload-peer	Reload the standby NI-2 card.
redundancy switch-activity	Switch over manually from the active NI-2 card to the standby NI-2 card.
show redundancy states	Display the state of the primary and secondary NI-2s, and identify which NI-2 is active.

redundancy switch-activity

To switch over manually from the active NI-2 card to the standby NI-2 card, use the **redundancy switch-activity** privileged EXEC command.

redundancy switch-activity

Syntax Description

This command has no argument or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Usage Guidelines

This command causes a manual switchover of activity to occur. This command also asks you for confirmation to save the running configuration if it has changed. If you enter "yes," the system saves the running command and then reloads all the cards in the chassis. If you enter "no," the system directly reloads all the cards in the chassis.

Examples

The command in the following example causes a manual switchover from the active NI-2 card to the standby NI-2 card:

```
DSLAM> enable
DSLAM# redundancy switch-activity
System configuration has been modified. Save? [yes/no]: no
This will reload the active unit and force a switch of activity. [confirm] y
```

Related Commands

Command	Description
redundancy reload-peer	Reload the standby NI-2 card.
redundancy reload-shelf	Reload all cards.
show redundancy states	Display the state of the primary and secondary NI-2s, and identify which NI-2 is active.

request-dialin

To configure an L2TP access concentrator (LAC) to request L2F or L2TP tunnels to an LNS and create a request-dialin VPDN subgroup, use the **request-dialin** VPDN group command. To remove the request-dialin subgroup from a VPDN group, use the **no** form of this command.

request-dialin

no request-dialin

Syntax Description

This command has no keywords nor arguments.

Defaults

Disabled

Command Modes

VPDN group mode

Command History

Release	Modification
12.2(1b) DA	This command was introduced.

Usage Guidelines

For a VPDN group to request dial-in calls, you must also configure the following commands:

- **initiate-to** VPDN group command
- **protocol** VPDN subgroup command
- At least one dialed number identification service (DNIS) or domain **request-dialin** command

After you establish an L2TP tunnel, both dial-in and dial-out calls can use the same tunnel.

Note You must configure the **vpdn-group** command with the **accept-dialin** command or the **request-dialin** command to enable VPDN. The **request-dialin** command initiates a dial-in tunnel. The acceptor, in turn, accepts a request for a dial-in tunnel.

Examples

The following example requests an L2TP dial-in tunnel to a remote peer at IP address 172.17.33.125 for a user in the domain named partner.com:

```
DSLAM(config)# vpdn-group 1
DSLAM(config-vpdn)# request-dialin
DSLAM(config-vpdn-req-in)# protocol l2tp
DSLAM(config-vpdn-req-in)# domain partner.com
DSLAM(config-vpdn-req-in)# initiate-to ip 172.17.33.125
```

Related Commands

Command	Description
accept-dialin	Accepts requests to create either L2F or L2TP tunnels for dial-in.
domain-name	Specifies the domain name for a DHCP client.
initiate-to	Specifies the IP address to which calls are tunneled.
multilink	Limits sessions that are authorized for all multilink users.
protocol	Specifies the tunneling protocol that is used for the dial-in connections.

route-target

To create a route-target extended community for a VRF, use the **route-target VRF submode** command. To disable the configuration of a route-target community option, use the **no** form of this command.

route-target {**import | export | both**} *route-target-ext-community*

no route-target {**import | export | both**} *route-target-ext-community*

Syntax Description

import	Import routing information from the target VPN extended community.
export	Export routing information to the target VPN extended community.
both	Import routing information from and export routing information to the target VPN extended community.
route-target-ext-community	Add the route-target extended community attributes to the VRF list of import, export, or both (import and export) route-target extended communities.

Defaults

There are no defaults. A VRF is not associated with any route-target extended community attributes until you specify the VRF using the **route-target** command.

Command Modes

VRF submode

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

The **route-target** command creates lists of import and export route target extended communities for the specified VRF. Execute the command one time for each target community. All VRFs that are configured with that extended community as an import route target contain learned routes that carry a specific route-target extended community. Learned routes from a VRF site (for example, by BGP, RIP, or static route configuration) contain export route targets for extended communities that are configured for the VRF added as route attributes to control the VRFs into which the route is imported.

The route-target specifies a target VPN extended community. Like a route-distinguisher, an extended community is composed of either an autonomous system number and an arbitrary number, or an IP address and an arbitrary number. You can enter the numbers in either of these formats:

- *16-bit AS number: your 32-bit number*
  For example, 101:3
- *32-bit IP address: your 16-bit number*
  For example, 192.168.122.15:1

Examples

The following example shows how to configure route-target extended community attributes for a VRF:

```
DSLAM(config)# ip vrf vrf_blue
DSLAM(config-vrf)# route-target both 1000:1
DSLAM(config-vrf)# route-target export 1000:2
DSLAM(config-vrf)# route-target import 173.27.0.130:200
```

Note The result of the command sequence is that VRF *vrf_blue* has two export extended communities (1000:1 and 1000:2) and two import extended communities (1000:1 and 173.27.0.130:200).

Related Commands

Command	Description
ip vrf	Enters VRF configuration mode.
import map	Configures an import route map for the VRF.

scrambling

To configure scrambling on an interface, use the **scrambling** interface configuration command. To restore the default value, use the **no** form of this command.

scrambling [**cell-payload | sts-stream**] [**protection | working | <cr>**]

no scrambling

Syntax Description

cell-payload	The 48-byte portion of an ATM cell carrying user data.
sts-stream	The portion of the Synchronous Transport Signal (STS) frame that carries user data (OC-3 only).
protection	The fiber that is connected to the NI-2 card in slot 11.
working	The fiber that is connected to the NI-2 card in slot 10.
<cr>	Both protection and working fibers.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(4)DA	This command was introduced.
12.1(7)DA	The keywords **protection** and **working** were added.

Usage Guidelines

The scrambling type must match on both sides of a link. Use the **scrambling** command only on trunk or subtend interfaces.

Examples

The following example uses the **scrambling** command to enable scrambling on the specified interface:

```
DSLAM> enable
DSLAM# configure terminal
DSLAM(config)# interface atm 0/1
DSLAM(config-if)# scrambling cell-payload protection
```

Note The **scrambling sts-stream** and **scrambling cell-payload** commands execute only on STS network interfaces such as OC-3.

Related Commands

Command	Description
payload scrambling	Enables ATM cell payload scrambling on a subscriber port.
show controllers	Displays information on working and protection fibers.

sdsl bitrate

To set the maximum and minimum allowed bit rates for the STU-C profile parameters, use the **sdsl bitrate** command.

sdsl bitrate *bitrate*

Syntax Description

bitrate	The STU-C upstream and downstream bit rates are identical. The loop characteristics determine the achievable rate. See the allowed ranges and default values in Usage Guidelines below.

Defaults

The default setting specifies a line rate of 784 kbps.

Command Modes

Profile configuration

Command History

Release	Modification
12.1(1)DA	This command was introduced.

Usage Guidelines

SDSL cards train only at the selected bit rate. If a CPE fails to train, a lower bit rate might be required.

The following allowable STU-C bit rate ranges occur in kilobits per second:

- 1168
- 1040
- 784
- 528
- 400
- 272
- 144

Caution This command causes the port to retrain when you change the bit rate parameter.

If you set a parameter to its current value, the port does not retrain. If a port is training when you change the parameter, the port untrains and retrains to the new parameter.

Examples

In this example, the command sets the bit rate of the default profile to 528 kbps downstream and upstream:

```
DSLAM# configure terminal
DSLAM(config)# dsl-profile default
DSLAM(cfg-dsl-profile)# sdsl bitrate 528
```

Related Commands

Command	Description
show dsl interface atm *slot#/port#*	Displays DSL and ATM status for a port.

secondary sync bootflash

To manually synchronize the bootflash files between the active and the standby NI-2, use the **secondary sync bootflash** privileged EXEC command.

secondary sync bootflash

Syntax Description

This command has no argument or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Usage Guidelines

Use this command to manually synchronize the bootflash files between the active and the standby NI-2. The **auto-sync** command performs this task automatically.

Examples

The following example synchronizes the bootflash files between the active and the standby NI-2:

```
DSLAM> enable
DSLAM# secondary sync bootflash
```

Related Commands

Command	Description
auto-sync	Automatically synchronizes the startup configuration between the active and the standby NI-2.
dir bootflash	Displays the bootflash files for the active NI-2 card.
dir secondary-bootflash	Displays the bootflash files for the standby NI-2 card.
secondary sync config	Synchronizes the startup configuration between the active and the standby NI-2.
secondary sync flash	Synchronizes the flash files from the active to the standby NI-2.
secondary sync running-config	Synchronizes the running configuration between the active and the standby NI-2.

secondary sync config

To manually copy the startup configuration and the IfIndex-table files from the active to the standby NI-2, use the **secondary sync config** privileged EXEC command.

secondary sync config

Syntax Description

This command has no argument or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Usage Guidelines

Use this command to manually copy the startup configuration from the active to the standby NI-2.

Examples

The command in the following example copies the startup configuration from the active to the standby NI-2:

```
DSLAM> enable
DSLAM# secondary sync config
```

Related Commands

Command	Description
auto-sync	Automatically synchronizes the startup configuration between the active and the standby NI-2.
dir bootflash	Displays the bootflash files for the active NI-2 card.
dir secondary-bootflash	Displays the bootflash files for the standby NI-2 card.
secondary sync bootflash	Synchronizes the bootflash files between the active and the standby NI-2.
secondary sync flash	Synchronizes the flash files between the active and the standby NI-2.
secondary sync running-config	Synchronizes the running configuration between the active and the standby NI-2.
show running-config	Displays the running configuration for every currently defined profile, including the default.
show startup-config	Displays the configuration file pointed to by the config_file environment variable.
squeeze	Deletes files and frees up space.

secondary sync flash

To manually synchronize the flash files on the active and the standby NI-2, use the **secondary sync flash** privileged EXEC command.

secondary sync flash

Syntax Description

This command has no argument or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Usage Guidelines

Use this command to manually synchronize the flash files on the active and the standby NI-2.

Examples

The following example synchronizes the flash files on the active and the standby NI-2:

```
DSLAM> enable
DSLAM# secondary sync flash
```

Related Commands

Command	Description
auto-sync	Automatically synchronizes the startup configuration on the active and the standby NI-2.
dir flash	Displays the flash files for the active NI-2 card.
dir secondary-flash	Displays the flash files for the standby NI-2 card.
secondary sync bootflash	Synchronizes the bootflash files on the active and the standby NI-2.
secondary sync config	Synchronizes the startup configuration on the active and the standby NI-2.
secondary sync running-config	Synchronizes the running configuration on the active and the standby NI-2.
squeeze	Deletes files and frees up space.

secondary sync running-config

To synchronize the running configurations on the active and the standby NI-2, use the **secondary sync running-config** privileged EXEC command.

secondary sync running-config

Syntax Description

This command has no argument or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Usage Guidelines

Use this command to synchronize the running configurations on the active and the standby NI-2.

Examples

The following example synchronizes the running configurations on the active and the standby NI-2:

```
DSLAM> enable
DSLAM# secondary sync running-config
```

Related Commands

Command	Description
auto-sync	Automatically synchronizes the startup configuration on the active and the standby NI-2.
secondary sync bootflash	Synchronizes the bootflash files on the active and the standby NI-2.
secondary sync config	Synchronizes the startup configuration on the active and the standby NI-2.
secondary sync flash	Synchronizes the flash files on the active and the standby NI-2.
show running-config	Displays the running configuration for every currently defined profile, including the default.
show startup-config	Displays the configuration file to which the config_file environment variable points.
squeeze	Deletes files and frees up space.

service dhcp

To enable the Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server feature, use the **service dhcp** global configuration command. Use the **no** form of this command to disable the Cisco IOS DHCP Server feature.

service dhcp

no service dhcp

Syntax Description

This command has no keywords or arguments.

Defaults

The feature is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

By default, the Cisco IOS DHCP Server feature is enabled on your Cisco DSLAM.

Examples

The following example enables DHCP services on the DHCP server:

```
DSLAM(config)# service dhcp
```

Related Commands

None.

set temperature-rating

Use the **set temperature-rating** command in EXEC mode to provision the system temperature rating.

set temperature-rating { *commercial* | *osp* **}**

Syntax Description

commercial	Commercial environment
osp	Outside-plant environment

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2(5)DA	This command was introduced.

Usage Guidelines

Use this command to set the temperature rating for the system. By default, system temperature ratings are set as commercial. A temperature rating mismatch alarm is triggered when any installed system component has a different temperature rating than the system temperature rating setting.

If the system temperature rating setting is osp, then any system component with a temperature rating of commercial triggers the temperature rating mismatch alarm. If the system temperature rating setting is commercial, then any system component with an osp rating triggers the alarm.

If a system has an osp rating but has never been provisioned, then the temperature rating mismatch alarm is on. To remove the alarm, set the system temperature rating to osp. When you change the system temperature rating setting, the facility-alarm status automatically updates, preventing unnecessary mismatch alarms.

Examples

The following examples show how to use the command to change the system temperature rating setting.

To set the system temperature rating to osp:

```
DSLAM> set temperature-rating osp
```

To set the system temperature rating to commercial:

```
DSLAM# set temperature-rating commercial
```

Related Commands

Command	Description
show environment	Displays information about system temperature settings, as well as temperature details for installed cards or recently provisioned card slots.
show facility-alarm status	Displays information about current alarms on your system.

shdsl annex

To configure the shdsl annex type, use the **shdsl annex** DSL profile configuration command. To disable, use the **no** form of this command.

shdsl annex {*a* | *b* | *auto*}

no shdsl annex {*a* | *b* | *auto*}

Syntax Description

a	Configures annex type a on the selected DSL profile.
b	Configures annex type b on the selected DSL profile.
auto	Allows the CO to detect and then select the CPE side annex type during training.

Defaults

The default setting for the **shdsl annex** command is auto.

Command Modes

DSL profile configuration.

Command History

Release	Modification
12.1(7)DA2	This command was introduced.
12.2(7)DA	The Auto Annex feature was added to the command.

Usage Guidelines

Use Annex A in North American network implementations. Annex B is appropriate for European shdsl implementations.

Examples

The following example shows how to configure shdsl Annex B:

```
DSLAM(config)# dsl-profile austin
DSLAM(cfg-dsl-prof)# shdsl annex b
```

Related Commands

Command	Description
shdsl set bitrate *rate* **masktype** *symmetric* **annex** {*a* | *b* | *auto*} **ratemode** {*fixed* | *adaptive*}	Configures the bit rate, mask type, annex type, and rate mode on a DSL profile.
shdsl margin {min *dB* | **threshold** *dB* | **target** *dB*}	Configures margin values, in decibels, on a DSL profile.

shdsl bitrate

To configure the shdsl bit rate, use the **shdsl bitrate** DSL profile configuration command. To disable, use the **no** form of this command.

shdsl bitrate *rate*

no shdsl bitrate

Syntax Description

rate	Specifies the maximum symmetrical data transmission rate for a G.SHDSL link. Valid rates are 72, 136, 200, 264, 392, 520, 776, 1032, 1160, 1544, 2056, and 2312 kbps.

Defaults

no shdsl bitrate

The default setting specifies a line rate of 776 kbps.

Command Modes

DSL profile configuration

Command History

Release	Modification
12.1(7)DA2	This command was introduced.

Usage Guidelines

If you change the bit rate on a live port, the line retrains.

Examples

The following example shows how to use the **shdsl bitrate** command to configure the upstream and downstream bandwidth at 2312 kbps:

```
DSLAM(config)# dsl-profile austin
DSLAM(cfg-dsl-prof)# shdsl bitrate 2312
```

Related Commands

Command	Description
shdsl set bitrate *rate* **masktype** *symmetric* **annex** {*a* | *b* | *auto*} **ratemode** {*fixed* | *adaptive*}	Configures the bit rate, mask type, annex type, and rate mode on a DSL profile.
shdsl margin {**min** *dB* | **threshold** *dB* | **target** *dB*}	Configures margin values, in decibels, on a DSL profile.

shdsl margin

To configure shdsl margins, use the **shdsl margin** DSL profile configuration command. To disable, use the **no** form of this command.

shdsl margin target *dB*

shdsl margin min *dB*

shdsl margin threshold *dB*

no shdsl margin target

no shdsl margin min

no shdsl margin threshold

Syntax Description

target	In rate adaptive mode, the target margin determines the amount of margin that is required before the line trains. If the line cannot achieve the target margin, it attempts to train at a lower rate. The line continues to lower the rate until it finds a line rate that supports the target margin.
dB	0 to 15 is the configurable range of values in decibels.
min	Configures the minimum SNR margin for the selected DSL profile. If the SNR falls below the configured value after the line has been trained for 5 seconds, the line drops and attempts to retrain.
dB	0 to 31 is the configurable range of values in decibels.
threshold	Configures the minimum SNR threshold margin. If the SNR margin falls below the configured value, an SNR margin threshold alarm is issued.
dB	0 to 31 is the configurable range of values in decibels.

Defaults

The default setting, **no shdsl margin** configures the following threshold values:

- **min**—0
- **threshold**—3
- **target**—0 (for rate adaptive mode the target default is 2)

Note We suggest using the **no shdsl margin** default settings.

Command Modes

DSL profile configuration.

Command History

Release	Modification
12.1(7)DA2	This command was introduced.

Usage Guidelines

Changing the shdsl margin on a live port causes the line to retrain.

Examples

The following example shows you how to configure the shdsl margin values **min** 2, **threshold** 10, and **target** 0:

```
DSLAM(config)# dsl-profile austin
DSLAM(cfg-dsl-prof)# shdsl margin min 2
DSLAM(cfg-dsl-prof)# shdsl margin threshold 10
DSLAM(cfg-dsl-prof)# shdsl margin target 0
```

Related Commands

Command	Description
shdsl set bitrate *rate* **masktype** *symmetric* **annex** {*a* | *b* | *auto*} **ratemode** {*fixed* | *adaptive*}	Configures the bit rate, mask type, annex type, and rate mode on a DSL profile.

shdsl masktype

To set the G.SHDSL mask type, use the **shdsl masktype** command in DSL profile configuration mode. To use the default mask type, use the **no** form of this command.

shdsl masktype *masktype*

no shdsl masktype

Syntax Description

symmetric	Configures symmetric mask type in the selected DSL profile.

Defaults

The default **shdsl masktype** is symmetric.

Command Modes

DSL profile configuration.

Command History

Release	Modification
12.1(7)DA2	This command was introduced.

Usage Guidelines

If you change the shdsl mask type on a live port, the line retrains.

Examples

The following example shows you how to configure a symmetric mask type:

```
DSLAM(config)# dsl-profile austin
DSLAM(cfg-dsl-prof)# shdsl masktype symmetric
```

Related Commands

Command	Description
shdsl set bitrate *rate* **masktype** *symmetric* **annex** {*a* | *b* | *auto*} **ratemode** {*fixed* | *adaptive*}	Configures the bit rate, mask type, annex type, and rate mode on a DSL profile.
shdsl margin {**min** *dB* | **threshold** *dB* | **target** *dB*}	Configures margin values, in decibels, on a DSL profile.

shdsl ratemode

To configure the type of training rate (fixed or adaptive), use the **shdsl ratemode** command. To disable ratemode, use the **no** form of this command.

shdsl ratemode {**fixed** | **adaptive**}

no shdsl ratemode

Syntax Description

fixed	In fixed training mode, no rates are negotiated. The line rate selected is the line rate to which the port attempts to train. If the port is unable to attain that line rate, it does not train.
adaptive	In adaptive training mode, the rate is negotiated during training. If the line cannot train at the selected rate, the line trains at the next best rate. Rates are negotiated in 64-kbps decrements.

Defaults

The default, **no shdsl ratemode**, is fixed.

Command Modes

DSL profile configuration.

Command History

Release	Modification
12.2(7)DA	This command was introduced.

Usage Guidelines

Changing the shdsl bit rate, mask type, rate, or annex type on a live port causes the line to retrain.

Examples

In the following example the training mode is configured as adaptive:

```
DSLAM(config)# dsl-profile austin
DSLAM(cfg-dsl-prof)# shdsl ratemode adaptive
```

Related Commands

Command	Description
shdsl annex {*a* | *b*}	Configures the annex type on a DSL profile.
shdsl bitrate *rate*	Configures the bit rate on a DSL profile.
shdsl masktype *symmetric*	Configures the mask type on a DSL profile.
shdsl margin {**min** *dB* | **threshold** *dB* | **target** *dB*}	Configures margin values, in decibels, on a DSL profile.
shdsl set bitrate *rate* **masktype** *symmetric* **annex** {*a* | *b* | *auto*}**ratemode** {*fixed* | *adaptive*}	Configures the bit rate, mask type, annex type, and ratemode on a DSL profile.

shdsl set bitrate masktype annex

The **shdsl set bitrate masktype annex** ratemode command aggregates the configuration of shdsl bit rates, mask types, annex types, and rate mode. To configure SHDSL bit rates, mask types, annex types, and rate mode, use the **shdsl set bitrate masktype annex ratemode** command in DSL profile configuration mode. To disable the **shdsl set bitrate masktype annex ratemode** command, use the **no** form of this command.

shdsl set bitrate *rate* **masktype** *symmetric* **annex** {*a* | *b* | *auto*} **ratemode {***fixed* | *adaptive***}**

no shdsl set bitrate masktype annex ratemode

Syntax Description

bitrate	Specifies the maximum symmetrical data transmission rate for a G.SHDSL link.
rate	Valid rates are 72, 136, 200, 264, 392, 520, 776, 1032, 1160, 1544, 2056, and 2312 kbps.
masktype	Configures the shdsl mask type for the selected DSL profile.
symmetric	Configures a symmetric mask type for the selected DSL profile.
annex	Configures the annex type for the selected DSL profile.
a	Configures Annex A for the selected DSL profile.
b	Configures Annex B for the selected DSL profile.
auto	Allows the CO to detect and then select the CPE side annex type during training.
ratemode	Configures the shdsl rate type for the selected DSL profile.
fixed	Configures a fixed training rate for the selected DSL profile.
adaptive	Configures an adaptive training rate for the selected DSL profile.

Defaults

The default **no shdsl set bitrate** *rate* **masktype** *symmetric* **annex** {*a* | *b* | *auto*} **ratemode** {*fixed* | *adaptive*} configures the following values on the selected DSL profile:

- Bit rate—776
- Mask type—Symmetric
- Annex—A
- Rate mode—(fixed)

Command Modes

DSL profile configuration.

Command History

Release	Modification
12.1(7)DA2	This command was introduced.
12.2(7)DA	The ratemode keyword was added.

Usage Guidelines

Changing the shdsl bit rate, mask type, rate, or annex type on a live port causes the line to retrain.

Examples

The following example shows how to configure a DSL profile with a 1544 kbps bit rate, symmetric mask type, Annex A, and adaptive rate mode:

```
DSLAM(config)# dsl-profile austin
DSLAM(cfg-dsl-prof)# shdsl set bitrate 1544 masktype symmetric annex a ratemode adaptive
```

Related Commands

Command	Description
shdsl annex {*a* | *b* | *auto*}	Configures the annex type on a DSL profile.
shdsl bitrate *rate*	Configures the bit rate on a DSL profile.
shdsl masktype *symmetric*	Configures the mask type on a DSL profile.
shdsl margin {**min** *dB* | **threshold** *dB* | **target** *dB*}	Configures margin values, in decibels, on a DSL profile.
shdsl ratemode {*fixed* | *adaptive*}	Configures the type of ratemode (fixed or adaptive) on a DSL profile.

Show Commands for Cisco DSLAMs with NI-2

This chapter documents commands you use to configure Cisco DSLAMs with NI-2. Commands in this chapter are listed alphabetically. For information on how to configure DSL features, refer to the *Configuration Guide for Cisco DSLAMs with NI-2*.

Note Commands that are identical to those documented in the *Cisco IOS Configuration Fundamentals Command Reference* and the *ATM and Layer 3 Switch Router Command Reference* have been removed from this chapter.

This chapter discusses the following commands:

show aps

show atm connection-traffic-table

show atm pvc

show atm vc

show atm vp

show cns config

show cns event

show controllers atm

show dsl interface

show dsl profile

show dsl status

show dsl status cap

show dsl status dmt

show dsl status idsl

show dsl status sdsl

show dsl status shdsl

show dsl test bert idsl

show environment

show facility-alarm status

show hardware

show hosts
show ima interface
show interfaces
show ip bgp vpnv4
show ip cef vrf
show ip dhcp binding
show ip dhcp conflict
show ip dhcp database
show ip dhcp server statistics
show ip protocols vrf
show ip route vrf
show ip vrf
show oir status
show redundancy states
show running-config
show smb
show snmp
show tag-switching forwarding vrf

show aps

To display the APS status of each SONET port on both NI-2 cards, use the **show aps** privileged EXEC command.

show aps [data]

Syntax Description

data	More detailed information on the APS status of each SONET port.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Usage Guidelines

This command displays the APS status of each SONET port. The Channel stat field displays the status of APS priority requests and failures. The priority-request commands, shown from highest to lowest level include:

1. **aps lockout**
2. **aps force**
3. **Signal Fail**
4. **aps manual**

A higher priority command executes even after you issue a lower priority command. However, a command of equal or lesser priority does not execute until you issue an **aps clear** command.

Table 6-1 describes the fields shown in the display.

Table 6-1 show aps Field Description

Field	Description
APS	This interface is operating in APS mode (default configuration).
Lin	This interface is operating in linear mode (default configuration).
NR	This interface is operating in nonrevertive mode (default configuration).
Uni	This interface is operating in unidirectional mode (default configuration).
Failure channel:	The inactive channel is either the working or the protection channel.
Active channel:	The active channel is either the working or the protection channel.

Table 6-1 show aps Field Description (continued)

Field	Description
Channel stat:	Signal Fail = failure on either of the fibers. Forced Switch = **aps force** command issued. Manual Switch = **aps manual** command issued. Lockout = **aps lockout** command issued. Good = **aps clear** command issued and both signals are good.
Port stat:	The signal/alarm status of the interface = Good, LOS, LOF, RDI, AIS, OOCD, LOP, APS mode mismatch, invalid (interface down).

Examples

The following example is sample output from the **show aps** privileged EXEC command:

```
DSLAM> enable
DSLAM# show aps
ATM0/1: APS Lin NR Uni, Failure channel: Protection
        Active Channel: Working, Channel stat: Good
        Port stat (w,p): (Good Signal, Good Signal)

ATM0/2: APS Lin NR Uni, Failure channel: Protection
        Active Channel: Working, Channel stat: Good
        Port stat (w,p): (Good Signal, Good Signal)
```

The following example is sample output from the **show aps data** privileged EXEC command:

```
DSLAM> enable
DSLAM# show aps data
ApsState struct:
apsEnabled         = TRUE
localLink          = PROTECTION
peerLink           = WORKING
peerPresent        = FALSE
peerCommUp         = FALSE
initialSwitchStateMsgReceived         = FALSE
PORT: P1
linkExists     = TRUE
auto-laser-control ON
local laser OFF
peer laser ON
activeLink     = WORKING
lockout        = FALSE
apsCommand     = 0
statsRecvd         = FALSE
ifIndex            = 0
currentState for WORKING          = DOWN
currentApsPortEvent for WORKING   = -1
currentState for PROTECTION          = DOWN
currentApsPortEvent for PROTECTION   = 12
PORT: P2
linkExists     = TRUE
auto-laser-control OFF
local laser ON
peer laser ON
activeLink     = PROTECTION
lockout        = FALSE
apsCommand     = 0
statsRecvd         = FALSE
```

```
ifIndex            = 0
currentState for WORKING          = DOWN
currentApsPortEvent for WORKING   = -1
currentState for PROTECTION          = AVAILABLE
currentApsPortEvent for PROTECTION   = 0
```

Related Commands

Command	Description
show controllers	Displays information on working and protection fibers.

show atm connection-traffic-table

To display a table of connection traffic parameters used by network and connection management, use the **show atm connection-traffic-table** EXEC command.

show atm connection-traffic-table [row *row-index* **| from-row** *row-index***]**

Syntax Descriptions

row	Displays a single row by the row-index number.
from-row	Displays the entire connection traffic table starting with the row-index.
row-index	Index of the single or starting row, in the range of 1 through 2147483647.

Defaults

Display the entire connection traffic table.

Command Modes

EXEC

Command History

Release	Modification
11.3(3a)	This command was introduced.

Usage Guidelines

An asterisk (*) is appended to row indexes created by SNMP but not made active. Because these rows are not active, they cannot be used by connections.

Examples

The following example shows sample output from the **show atm connection-traffic-table** command.

```
DSLAM# show atm connection-traffic-table
Row      Service-category    pcr        scr/mcr       mbs         cdvt   name
1            ubr           7113539        none                     none
2            cbr              424                                 none
3            vbr-rt           424         424          50         none
4            vbr-nrt          424         424          50         none
5            abr              424        none                     none
6            ubr              424        none                     none
200          cbr             7743        none                     none   traffic-row1
64000        cbr             1741                                 none
2147483645*  ubr                0        none                     none
2147483646*  ubr                1        none                     none
2147483647*  ubr           7113539        none                     none
```

Table 6-2 describes the significant fields shown in the display.

Table 6-2 show atm connection-traffic-table Field Descriptions

Field	Description
row	Index to the connection traffic table.
service-category	One of the following: **ubr** **cbr** **vbr-rt** **vbr-nrt** **abr**
pcr	The value of the peak cell rate. The peak cell rate is measured in kbps, and is used to transmit whole cells, including the header.
scr/mcr	The value of the sustained cell rate/maximum cell rate. These values are measured in kbps, and are used to transmit whole cells, including the header.
mbs	The value of the mbs.
name	The name for the traffic table row.
cdvt	The value of the cell delay variation tolerance.

Related Commands

Command	Description
atm connection-traffic-table-row	Displays information on working and protection fibers.

show atm pvc

To display all ATM PVCs and traffic information, use the **show atm pvc** privileged EXEC command.

show atm pvc [*ppp*]

Syntax Description

ppp	Displays each PVC configured for PPP over ATM.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

If you do not specify *vpi*/*vci* or *name*, the output of this command is the same as that of the **show atm vc** command, but only the configured PVCs display.

Examples

The following is sample output from the **show atm pvc** command:

```
DSLAM> show atm pvc

VCD /                                        Peak  Avg/Min Burst
Interface   Name       VPI   VCI  Type   Encaps   SC   Kbps   Kbps   Cells  Sts
0/1         37          0     5   PVC    SAAL     UBR  155000000             IC
0/1         35          0    16   PVC    ILMI     UBR  155000000             IC
0/1         39          0    18   PVC    UBR      ILMI 155000000             INAC
0/2         38          0     5   PVC    SAAL     UBR  155000000             IC
0/2         36          0    16   PVC    ILMI     UBR  155000000             IC
```

Table 6-3 describes the significant fields in the example.

Table 6-3 show atm pvc Field Descriptions

Field	Description
Interface	Interface slot number and port number.
VCD/Name	Virtual circuit descriptor (virtual circuit number). The connection name displays if you configure a name for the virtual channel with the **pvc** command.
VPI	Virtual path identifier.
VCI	Virtual channel identifier.

Table 6-3 show atm pvc Field Descriptions (continued)

Field	Description
Type	Type of PVC detected from PVC discovery, either PVC-D, PVC-L, or PVC-M. PVC-D indicates a PVC created due to PVC discovery. PVC-L indicates that the corresponding peer of this PVC was not found on the DSLAM. PVC-M indicates that some or all of the QoS parameters of this PVC mismatch those of the corresponding peer on the DSLAM.
Encaps	Type of ATM adaptation layer (AAL) and encapsulation.
Peak or PeakRate	Kilobits per second transmitted at the peak rate.
Avg/Min or Average Rate	Kilobits per second transmitted at the average rate.
Burst Cells	Value that equals the maximum number of ATM cells that the virtual circuit can transmit at peak rate.
Sts or Status	Status of the virtual channel connection. UP indicates that the connection is enabled for data traffic. DOWN indicates that the connection is not ready for data traffic. When the Status field is DOWN, a State field is shown. See a description of the different values for this field listed later in this table. INACTIVE indicates that the interface is down.
Connection Name	The name of the PVC.
UBR, UBR+, or VBR–NRT	UBR—Unspecified Bit Rate QoS is specified for this PVC. See the **ubr** command for further information. UBR+—Unspecified Bit Rate QoS is specified for this PVC. See the **ubr+** command for further information. VBR–NRT—Variable Bit Rate–Non Real Time QoS rates are specified for this PVC. See the **vbr-nrt** command for further information.
etype	Encapsulation type.

Table 6-3 show atm pvc Field Descriptions (continued)

Field	Description
Flags	Bit mask that describes virtual circuit information. The flag values are summed to result in the displayed value. 0x40—SVC 0x20—PVC 0x10—ACTIVE 0x0—AAL5-SNAP 0x1—AAL5-NLPID 0x2—AAL5-FRNLPID 0x3—AAL5-MUX 0x4—AAL3/4-SMDS 0x5—QSAAL 0x6—ILMI 0x7—AAL5-LANE 0x9—AAL5-CISCOPPP
virtual-access	Virtual access interface identifier.
virtual-template	Virtual template identifier.
VCmode	AIP-specific or NPM-specific register that describes the usage of the virtual circuit. This register contains values such as rate queue, peak rate, and AAL mode, which also display in other fields.
OAM frequency	Number of seconds between the sending of OAM loopback cells.
OAM retry frequency	The frequency (in seconds) that end-to-end F5 loopback cells transmit when the software verifies a change in UP/DOWN state. For example, if a PVC is up and the software does not receive a loopback cell response after the *frequency* (in seconds) that you specify using the **oam-pvc** command, then the software sends loopback cells at the *retry-frequency* to verify whether the PVC is down.
OAM up retry count	Number of consecutive end-to-end F5 OAM loopback cell responses that the software must receive to change a PVC state to up. Does not apply to SVCs.
OAM down retry count	Number of consecutive end-to-end F5 OAM loopback cell responses that the software does not receive to change a PVC state to down or tear down an SVC.
OAM Loopback status	Status of end-to-end F5 OAM loopback cell generation for this virtual channel. This field has one of the following values: OAM Disabled—End-to-End F5 OAM loopback cell generation is disabled. OAM Sent—OAM cell was sent. OAM Received—OAM cell was received. OAM Failed—OAM reply was not received within the frequency period or contained a bad correlation tag.

Table 6-3 show atm pvc Field Descriptions (continued)

Field	Description
OAM VC state	This field has one of the following states for this virtual channel: AIS/RDI—The virtual channel received AIS/RDI cells. The software does not send end-to-end F5 OAM loopback cells in this state. Down Retry—An OAM loopback failed. The software does not send end-to-end F5 OAM loopback cells at retry frequency to verify whether the virtual channel is really down. After down-count unsuccessful retries, the virtual channel goes to the Not Verified state. Not Managed—OAM is not managing the virtual channel. Not Verified—End-to-end F5 OAM loopback cells did not verify the virtual channel. AIS and RDI conditions clear. Up Retry—An OAM loopback was successful. The software sends end-to-end F5 OAM loopback cells at retry frequency to verify that the virtual channel is really up. After up-count successive and successful loopback retries, the virtual channel goes to the Verified state. Verified—Loopbacks are successful. The software did not receive an AIS/RDI cell.
ILMI VC state	This field has one of the following states for this virtual channel: Not Managed—ILMI did not manage the virtual channel. Not Verified—ILMI did not verify the virtual channel. Verified—ILMI verified the virtual channel.
VC is managed by OAM/ILMI	OAM and/or ILMI manage the virtual channel.
InARP frequency	Number of minutes for the Inverse ARP time period.
InPkts	Total number of packets received on this virtual circuit. This number includes all fast-switched and process-switched packets.
OutPkts	Total number of packets sent on this virtual circuit. This number includes all fast-switched and process-switched packets.
InBytes	Total number of bytes received on this virtual circuit. This number includes all fast-switched and process-switched bytes.
OutBytes	Total number of bytes sent on this virtual circuit. This number includes all fast-switched and process-switched bytes.
InPRoc	Number of process-switched input packets.
OutPRoc	Number of process-switched output packets.
Broadcasts	Number of process-switched broadcast packets.
InFast	Number of fast-switched input packets.
OutFast	Number of fast-switched output packets.
InAS	Number of autonomous-switched or silicon-switched input packets.
OutAS	Number of autonomous-switched or silicon-switched output packets.
OAM cells received	Total number of OAM cells received on this virtual circuit.
F5 InEndloop	Number of end-to-end F5 OAM loopback cells received.

Table 6-3 show atm pvc Field Descriptions (continued)

Field	Description
F5 InSegloop	Number of segment F5 OAM loopback cells received.
F5 InAIS	Number of F5 OAM AIS cells received.
F5 InRDI	Number of F5 OAM RDI cells received.
F4 InEndloop	Number of end-to-end F4 OAM loopback cells received.
F4 InSegloop	Number of segment F4 OAM loopback cells received.
F4 InAIS	Number of F4 OAM AIS cells received.
F4 InRDI	Number of F4 OAM RDI cells received.
OAM cells sent	Total number of OAM cells sent on this virtual circuit.
F5 OutEndloop	Number of end-to-end F5 OAM loopback cells sent.
F5 OutSegloop	Number of segment F5 OAM loopback cells sent.
F5 OutRDI	Number of F5 OAM RDI cells sent.
OAM cell drops	Number of OAM cells dropped (or flushed).

Table 6-3 show atm pvc Field Descriptions (continued)

Field	Description
PVC Discovery	NOT_VERIFIED—This PVC is manually configured on the router and not yet verified with the attached adjacent switch. WELL_KNOWN—This PVC has a VCI value of 0 through 31. DISCOVERED—This PVC is learned from the attached adjacent switch via ILMI. MIXED—Some of the traffic parameters for this PVC are learned from the switch through ILMI. MATCHED—This PVC is manually configured on the router, and the local traffic shaping parameters match the parameters learned from the switch. MISMATCHED—This PVC is manually configured on the router, and the local traffic shaping parameters do not match the parameters learned from the switch. LOCAL_ONLY—This PVC is configured locally on the router and not on the remote switch.
State	When the Status field is UP, this field does not appear. When the Status field is DOWN or INACTIVE, the State field appears with one of the following values: NOT_VERIFIED—The virtual channel has been established successfully; waiting for OAM (if enabled) and ILMI (if enabled) to verify that the virtual channel is up. NOT_EXIST—Virtual channel has not been created. HASHING_IN—Virtual channel has been hashed into a hash table. ESTABLISHING—Ready to establish virtual channel connection. MODIFYING—Virtual channel parameters have been modified. DELETING—Virtual channel is being deleted. DELETED—Virtual channel has been deleted. NOT_IN_SERVICE—ATM interface is shut down.

show atm vc

To display the ATM layer connection information about the virtual connection, use the **show atm vc** EXEC command.

show atm vc
show atm vc interface {**atm** | **atm-p**} *slot#/port#*[**.***vpt#*] [*vpi vci*] [**detail**]
show atm vc [**cast-type** *cast-type*] [**conn-type** *conn-type*] [**interface** {**atm** | **atm-p**} *slot#/port#*[**.***vpt#*]]
show atm vc traffic [**interface** {**atm** | **atm-p**} *slot#/port#*[**.***vpt#*] [*vpi vci*]]

Syntax Description

slot#/port#	Slot number and port number for the interface.
.*vpt#*	Virtual path tunnel identifier to display.
vpi vci	Virtual path identifier and virtual channel identifier to display.
detail	Displays the Rx cell drops and queued-cells for all virtual channels on a given interface.
cast-type	Specifies the cast type as multipoint-to-point (mp2p), point-to-multipoint (p2mp), or point-to-point (p2p).
conn-type	Specifies the connection type as **pvc**, **soft-vc**, **svc**, or **tvc**.
traffic	Displays the virtual channel cell traffic.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.2(5)DA	A failure cause code was added for soft virtual channels that are not connected.

Examples

The following example shows a display for the vc interface:

```
DSLAM# show atm vc

Interface     VPI   VCI    Type   X-Interface  X-VPI X-VCI   Encap  Status   Name
ATM0/1          0    5     PVC    ATM0/0          0     37    QSAAL  UP       con1
ATM0/1          0    16    PVC    ATM0/0          0     35    ILMI   UP       con2
ATM0/1          0    18    PVC    ATM0/0          0     39    PNNI   UP
```

Table 6-4 describes the significant fields shown in the displays.

Table 6-4 show atm vc Field Descriptions

Field	Description
Interface	Displays the slot number and port number of the specified ATM interface.
VPI	Displays the number of the virtual path identifier.

Table 6-4 show atm vc Field Descriptions (continued)

Field	Description
VCI	Displays the number of the virtual channel identifier.
Type	Displays the type of interface for the specified ATM interface.
X-Interface	Displays the slot number and port number of the cross-connected value for the ATM interface. Also displays a failure code for soft virtual channels that are not connected.
X-VPI	Displays the number of the cross-connected value of the virtual path identifier.
X-VCI	Displays the number of the cross-connected value of the virtual channel identifier.
Encap	Displays the type of connection on the interface.
Status	Displays the current state of the specified ATM interface.
Name	Displays the name of the PVC connection.

The following example shows the interface information for ATM 5/2, with VPI 1 and VCI 2:

```
DSLAM# show vc interface atm 5/2 1 2

 Interface: ATM5/2, Type: dsl
 VPI = 1  VCI = 2
 Status: NOT CONNECTED
 Connection-type: SoftVC
 Connection-Name: con1
 Cast-type: point-to-point
 Usage-Parameter-Control (UPC): pass
 Packet-discard-option: disabled
 Time-since-last-status-change: 00:17:33
  Soft vc location: Source
  Remote ATM address: 47.0091.8100.0000.00d0.5881.0401.4000.0c82.0010.00
  Remote VPI: 10
  Remote VCI: 111
  Soft vc call state: Inactive
  Number of soft vc re-try attempts: 21
  First-retry-interval: 5000 milliseconds
  Maximum-retry-interval: 60000 milliseconds
  Next retry in: 41964 milliseconds
  Last release cause: 35,requested VPCI/VCI not available
  Aggregate admin weight: 0
  TIME STAMPS:
  Current Slot:2
   Outgoing Setup     September 27 22:02:52.979
   Incoming Release   September 27 22:02:52.987
   Outgoing Setup     September 27 21:58:52.943
   Incoming Release   September 27 21:58:52.951
   Outgoing Setup     September 27 21:59:52.951
   Incoming Release   September 27 21:59:52.959
   Outgoing Setup     September 27 22:00:52.959
   Incoming Release   September 27 22:00:52.967
   Outgoing Setup     September 27 22:01:52.967
   Incoming Release   September 27 22:01:52.979
```

```
Number of OAM-configured connections: 0
OAM-configuration: disabled
OAM-states:  Not-applicable
Rx cells: 0, Tx cells: 0
Rx connection-traffic-table-index: 1
Rx service-category: UBR (Unspecified Bit Rate)
Rx pcr-clp01: 7113539
Rx scr-clp01: none
Rx mcr-clp01: none
Rx      cdvt: 1024 (from default for interface)
Rx       mbs: none
Tx connection-traffic-table-index: 1
Tx service-category: UBR (Unspecified Bit Rate)
Tx pcr-clp01: 7113539
Tx scr-clp01: none
Tx mcr-clp01: none
Tx      cdvt: none
Tx       mbs: none
```

Table 6-5 describes the fields shown in the displays.

Table 6-5 show atm vc interface ATM Field Descriptions

Field	Description
Interface	Displays the slot number and port number of the ATM interface.
VPI/VCI	Displays the number of the virtual path identifier and the virtual channel identifier.
Status	Displays the type of interface for the specified ATM interface.
Connection-type	Displays the type of connection for the specified ATM interface.
Connection-Name	Displays the name of the PVC connection.
Cast-type	Displays the type of cast for the specified ATM interface.
Usage-Parameter-Control (UPC)	Displays the state of the UPC.
Packet-discard-option	Displays the state of the packet-discard option; enabled or disabled.
Time-since-last-status-change	Displays the time elapsed since the last status change.
Soft vc location	Displays the Soft VC/Soft VP location for the ATM connection. The location can be either Source or Destination.
Remote ATM address	Displays the ATM address of the destination port.
Remote VPI	Displays the destination VPI number.
Remote VCI	Displays the destination VCI number.
Soft vc call state	Displays the state of the Soft VC/Soft VP. The call state can be Inactive, Initiating, Active, Releasing, Deleting, or Invalid.
Number of soft vc re-try attempts	Displays the number of retry attempts that have been made to open a Soft VC/Soft VP connection.

Table 6-5 show atm vc interface ATM Field Descriptions (continued)

Field	Description
First-retry-interval	Displays the interval for the first retry after the first failed attempt, specified in milliseconds. If the first retry after the first failed attempt also fails, subsequent attempts are made at intervals computed using the first retry-interval as follows: (2 ** (k–1)) * first retry-interval Where the value of *k* is 1 for the first retry after the first failed attempt and is incremented by 1 for every subsequent attempt. The range is from 100 to 3600000 milliseconds; the default is 5000 milliseconds.
Maximum-retry-interval	Displays the maximum retry interval between any two attempts, specified in seconds. Once the retry interval is computed in the first retry interval and becomes equal to or greater than the maximum retry interval configured, the subsequent retries are done at regular intervals of maximum retry-interval seconds until the call is established. Range is from 1 to 65535 seconds; the default is 60.
Next retry in	Displays the time interval for the next retry attempt, specified in milliseconds.
Last release cause	Displays the number and description string for the cause of the failure.
Aggregate admin weight	Displays the aggregate admin weight for the Soft VC/Soft VP connection.
TIME STAMPS	Displays the current slot and the time stamps of various states of the connection.
Number of OAM-configured connections	Displays the number of connections configured by OAM.
OAM-configuration	Displays the state of the OAM configuration, enabled or disabled.
OAM-states	Displays the status of the OAM state, applicable or not applicable.
Rx cells/Tx cells	Displays the number of cells transmitted and received.
Rx connection-traffic-table-index	Displays the receive connection-traffic-table-index.
Rx service-category	Displays the receive service category.
Rx pcr-clp01	Displays the receive peak cell rate for clp01 cells (kbps).
Rx scr-clp01	Displays the receive sustained cell rate for clp01 cells (kbps).
Rx mcr-clp01	Displays the receive minimum cell rate for clp01 cells (kbps).
Rx cdvt	Displays the receive cell delay variation tolerance.
Rx mbs	Displays the receive minimum burst size.
Tx connection-traffic-table-index	Displays the transmit connection-traffic-table-index.
Tx service-category	Displays the transmit service category.
Tx pcr-clp01	Displays the transmit peak cell rate for clp01 cells (kbps).
Tx scr-clp01	Displays the transmit sustained cell rate for clp01 cells (kbps).

Table 6-5 show atm vc interface ATM Field Descriptions (continued)

Field	Description
Tx mcr-clp01	Displays the transmit minimum cell rate for clp01 cells (kbps).
Tx cdvt	Displays the transmit cell delay variation tolerance.
Tx mbs	Displays the transmit minimum burst size.

Examples

The following example shows how to enter the command for a display of the cast type, point-to-multipoint, and connection type soft-vc on ATM 0/1.

```
DSLAM# show atm vc cast-type p2mp conn-type soft-vc interface atm0/1
```

The following example shows how to enter the command for a display of the connection type SVC and cast-type point-to-point on ATM interface 0/1.

```
DSLAM# show atm vc conn-type svc cast-type p2p interface atm0/1
```

The following example shows the transmit and receive cell count on ATM 0/1, with VPI 1 and VPI 100.

```
DSLAM# show atm vc traffic interface atm 0/1 1 100
Interface    VPI     VCI      Type      rx-cell-cnts     tx-cell-cnts
ATM0/1 1       100       PVC                0                0
```

Related Commands

Command	Description
atm pvc	Creates a PVC.
show atm interface	Displays ATM-specific information about an ATM interface.
show atm status	Displays current information about ATM interfaces and specifies the number of installed connections.

show atm vp

To display the ATM layer connection information about the virtual path, use the **show atm vp** EXEC command.

show atm vp

show atm vp interface atm *slot#/port#*[**.***vpt#*] [*vpi vci*]

show atm vp traffic [**interface** {**atm** | **atm-p**}slot#/*port#*[**.***vpt#*] [*vpi vci*]]

Syntax Description

interface atm	Shows ATM connection commands.
slot#/port#	Slot and port number for the interface.
.*vpt#*	Virtual path tunnel identifier.
vpi vci	Virtual path identifier and virtual channel identifier to display.
traffic	Displays the virtual channel cell traffic.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.2(5)DA	A failure cause code was added for soft PVPs that are not connected.

Examples

This example is sample output from the **show atm vp** command for ATM 0/1.

```
DSLAM> show atm vp
Interface     VPI    Type   X-Interface  X-VPI  Status   Name
ATM0/1        23     SVP     ATM5/3        1     UP       vpcon1
ATM5/3        1      SoftVP  ATM0/1        23    UP       vpcon2
ATM5/3        2      SoftVP  NOT CONNECTED (35)
```

This example is sample output from the **show vp interface atm** command for ATM5/3, with VPI 2.

```
DSLAM> show vp interface atm 5/3 2

Interface: ATM5/3, Type: dsl
 VPI = 2
 Status: NOT CONNECTED
 Time-since-last-status-change: 00:10:22
 Connection-type: SoftVP
 Cast-type: point-to-point
  Soft vp location: Source
  Remote ATM address: 47.0091.8100.0000.00d0.5881.0401.4000.0c82.0010.00
  Remote VPI: 9
  Soft vp call state: Inactive
  Number of soft vp re-try attempts: 14
  First-retry-interval: 5000 milliseconds
  Maximum-retry-interval: 60000 milliseconds
  Next retry in: 52388 milliseconds
  Last release cause: 35,requested VPCI/VCI not available
```

```
 Aggregate admin weight: 0
 TIME STAMPS:
 Current Slot:8
  Outgoing Setup     September 27 22:02:00.643
  Incoming Release   September 27 22:02:00.651
  Outgoing Setup     September 27 22:03:00.651
  Incoming Release   September 27 22:03:00.659
  Outgoing Setup     September 27 22:04:00.659
  Incoming Release   September 27 22:04:00.667
  Outgoing Setup     September 27 22:05:00.667
  Incoming Release   September 27 22:05:00.675
  Outgoing Setup     September 27 22:01:00.635
  Incoming Release   September 27 22:01:00.643

Usage-Parameter-Control (UPC): pass
Number of OAM-configured connections: 0
OAM-configuration: disabled
OAM-states:  Not-applicable
Rx cells: 0, Tx cells: 0
Rx connection-traffic-table-index: 1
Rx service-category: UBR (Unspecified Bit Rate)
Rx pcr-clp01: 7113539
Rx scr-clp01: none
Rx mcr-clp01: none
Rx      cdvt: 1024 (from default for interface)
Rx       mbs: none
Tx connection-traffic-table-index: 1
Tx service-category: UBR (Unspecified Bit Rate)
Tx pcr-clp01: 7113539
Tx scr-clp01: none
Tx mcr-clp01: none
Tx      cdvt: none
Tx       mbs: none
```

Table 6-6 describes the fields shown in the displays.

Table 6-6 show atm vp interface atm Field Descriptions

Field	Description
Interface	Displays the slot and port number of the ATM interface.
VPI	Displays the number of the virtual path identifier.
Status	Displays the type of interface for the specified ATM interface.
Time-since-last-status-change	Displays the time elapsed since the last status change.
Connection-type	Displays the type of connection for the specified ATM interface.
Cast-type	Displays the type of cast for the specified ATM interface.
Soft vc location	Displays the Soft VC/Soft VP location for the ATM connection. The location can be either Source or Destination.
Remote ATM address	Displays the ATM address of the destination port.
Remote VPI	Displays the destination VPI number.
Remote VCI	Displays the destination VCI number.
Soft vc call state	Displays the state of the Soft VC/Soft VP. The call state can be Inactive, Initiating, Active, Releasing, Deleting, or Invalid.
Number of soft vc re-try attempts	Displays the number of retry attempts made to open a Soft VC/Soft VP connection.

Table 6-6 show atm vp interface atm Field Descriptions (continued)

Field	Description
First-retry-interval	Displays the interval for the first retry after the first failed attempt, specified in milliseconds. If the first retry after the first failed attempt also fails, subsequent attempts are made at intervals computed using the first retry-interval as follows: (2 ** (k–1)) * first retry-interval Where the value of *k* is 1 for the first retry after the first failed attempt and is incremented by 1 for every subsequent attempt. The range is from 100 to 3600000 milliseconds; the default is 5000 milliseconds.
Maximum-retry-interval	Displays the maximum retry interval between any two attempts, specified in seconds. Once the retry interval is computed in the first retry interval and becomes equal to or greater than the maximum retry interval configured, the subsequent retries are done at regular intervals of maximum retry-interval seconds until the call is established. Range is from 1 to 65535 seconds; the default is 60.
Next retry in	Displays the time interval for the next retry attempt, specified in milliseconds.
Last release cause	Displays the number and description string for the cause of the failure.
Aggregate admin weight	Displays the aggregate admin weight for the Soft VC/Soft VP connection.
TIME STAMPS	Displays the current slot and the time stamps of various states of the connection.
Usage-Parameter-Control (UPC)	Displays the state of the UPC.
Number of OAM-configured connections	Displays the amount of connections configured by OAM.
OAM-configuration	Displays the state of the OAM configuration, enabled or disabled.
OAM-states	Displays the status of the OAM state, applicable or not applicable.
Rx cells/Tx cells	Displays the number of cells transmitted and received.
Rx connection-traffic-table-index	Displays the receive connection-traffic-table-index.
Rx service-category	Displays the receive service category.
Rx pcr-clp01	Displays the receive peak cell rate for clp01 cells (kbps).
Rx scr-clp01	Displays the receive sustained cell rate for clp01 cells (kbps).
Rx mcr-clp01	Displays the receive minimum cell rate for clp01 cells (kbps).
Rx cdvt	Displays the receive cell delay variation tolerance.
Rx mbs	Displays the receive maximum burst size.
Tx connection-traffic-table-index	Displays the transmit connection-traffic-table-index.
Tx service-category	Displays the transmit service category.
Tx pcr-clp01	Displays the transmit peak cell rate for clp01 cells (kbps).

Table 6-6 show atm vp interface atm Field Descriptions (continued)

Field	Description
Tx scr-clp01	Displays the transmit sustained cell rate for clp01 cells (kbps).
Tx mcr-clp01	Displays the transmit minimum cell rate for clp01 cells (kbps)
Tx cdvt	Displays the transmit cell delay variation tolerance.
Tx mbs	Displays the transmit maximum burst size.

Related Commands

Command	Description
show atm interface	Displays ATM-specific information about an ATM interface.
show atm status	Displays current information about ATM interfaces and the number of installed connections.

show cns config

To display information about the Cisco Networking Services (CNS) Configuration Agent, use the **show cns config** command in EXEC mode.

show cns config {**status** | **outstanding** | **stats**}

Syntax Description

status	Displays the status of the Configuration Agent. Use this option to display the following information about the Configuration Agent: • Status of the partial Configuration Agent; for example, whether it has been configured properly. • IP address and port number of the trusted server that the partial Configuration Agent is using. • Configuration ID, the unique ID for the Configuration Agent.
outstanding	Displays information about the outstanding configurations. An outstanding configuration is a partial configuration that has been started but not completed. Use this keyword to display information about the following outstanding partial configurations: • Queue ID of the configuration—An identifier of the configuration in the configuration queue. • Identifier—Along with the configuration ID, the identifier is used to uniquely identify each partial configuration. Typically this value can be used to define a group of configurations. • Configuration ID—Along with the identifier, the configuration ID is used to uniquely identify each partial configuration. Typically this value uniquely identifies configuration data within the group specified by the identifier.
stats	Displays the following statistics on the Configuration Agent: • The number of configurations completed • The number of configurations failed • The time stamp of the last configuration received

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2(5)DA	This command was introduced.

Usage Guidelines

Use this command to display information about the Configuration Agent.

Related Commands

Command	Description
cns config initial	Starts the initial CNS Configuration Agent.
cns config partial	Starts the partial CNS Configuration Agent.

show cns event

To display information about the Cisco Networking Services (CNS) Event Agent, use the **show cns event** command in EXEC mode.

show cns event {**status** | **subject** [*name*] | **gateway** | **stats**}

Syntax Description

status	Displays the following status information: • Status of Event Agent: – Connected – Active • Gateway used by the Event Agent: – IP address – Port number – Device ID
subject	Displays a list of subjects that are subscribed to by applications.
name	(Optional) Displays a list of applications that are subscribing to this specific subject name.
gateway	Displays the following information for the gateways: • Primary gateway: – IP address – Port number • Backup gateways: – IP address – Port number • Currently connected gateway: – IP address – Port number
stats	Displays the following statistics for the Event Agent: • Number of events received • Number of events sent • Number of events not processed successfully • Number of events in the queue • Time stamp of latest event received (time stamp is router time) • Time stamp of latest event sent • Number of applications using the Event Agent • Number of subjects subscribed

Defaults No default behavior or values.

Command Modes EXEC

Command History

Release	Modification
12.2(5)DA	This command was introduced.

Usage Guidelines Use this command to display information about the Event Agent.

Related Commands

Command	Description
cns event	Configures the CNS Event Gateway.

show controllers atm

To display debugging information for a port, use the **show controllers atm** command.

show controllers atm *slot#/port#*

Syntax Description

slot#/port#	The slot number and port number of the port for which you want to display debugging information. The slot range is 0 to 38. The port range is 1 to 8. (These are maximum ranges; your card might have fewer than 8 ports, and your chassis might have fewer than 39 slots.)

Defaults

There is no default value for this command.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

This command is primarily for engineering use.

The output for this command varies with the interface type. It provides low-level diagnostic information that is specific to the physical layer chipset.

Command output for a DMT interface; for example, includes these items:

- Absolute signal-to-noise ratio (SNR) for each of the upstream bins.
- Bit allocation for each of the upstream and downstream bins.

Note Output items for SDSL ports display one value for both upstream and downstream.

- Downstream transmit power boost (power spectral density mask, config, and actual). Autoconfigured power boost displays as a whole number of decibels. Actual power boost displays in decibels to one decimal place (0.1 dB) accuracy.
- The contents of these configuration management variable (CMV) chipsets include:
  - UOPT[7: 0] (upstream training options)
  - DOPT[7: 0] (downstream training options)
  - ADPT.downstream
  - ADPT.upstream
  - RATE.actual
  - RATE.maximum
  - CODE.upstream

- CODE.downstream
- INTL.upstream
- INTL.downstream
- DIAG.control
- DIAG.flags_latched
- PSDM.config
- PSDM.actual
- OPTN.options
- OPTN.bitswap
- OPTN.utopia

Examples

In this example, the command displays debugging information for ATM 0/1 and ATM 0/2:

```
DSLAM> show controllers atm 0/1
IF Name: ATM0/1    Chip Base Address: B3809000
Port type: OC3    Port rate: 155000 kbps    Port medium: MM Fiber

Alarms:
Source: ATM0/1 working  Severity: CRITICAL Description: 10   Loss of Signal

                                  local            peer
                                (working)       (protection)
                                 ACTIVE           INACTIVE
                              ---------------   ---------------
Port status                       SECTION LOS     Not available
Loopback                                None     Not available
Flags                                 0x8300     Not available
TX clock source                network-derived     Not available
Framing mode                          sts-3c     Not available
Cell payload scrambling                  On     Not available
Sts-stream scrambling                    On     Not available
TX Led:                                  On     Not available
RX Led:                                  On     Not available
TST Led:                                Off     Not available

OC3 counters:
  cells transmitted                    41785                0
  cells received                       44150                0
  cells sent to peer                   41785                0
  cells received from peer                 0                0
  section BIP-8 errors                     0                0
  line BIP-8 errors                        0                0
  path BIP-8 errors                        0                0
  OOCD errors (not supported)              0                0
  line FEBE errors                         0                0
  path FEBE errors                         0                0
  correctable HEC errors                   0                0
  uncorrectable HEC errors                 0                0

OC3 errored seconds:
  section BIP-8                            0                0
  line BIP-8                               0                0
  path BIP-8                               0                0
  OOCD (not supported)                     0                0
  line FEBE                                0                0
```

```
  path FEBE                                0                0
  correctable HEC                          0                0
  uncorrectable HEC                        0                0

OC3 error-free secs:
  section BIP-8                        88704                0
  line BIP-8                           88704                0
  path BIP-8                           88704                0
  OOCD (not supported)                     0                0
  line FEBE                            88704                0
  path FEBE                            88704                0
  correctable HEC                      88704                0
  uncorrectable HEC                    88704                0

                local   peer                      local   peer
                -----   ----                      -----   ----
Per chip registers
  mr             0x69   0x00   |   mmc             0x6B   0x00
  mcmr           0x6F   0x00   |   cscsr           0x54   0x00
  ictl           0x5F   0x00   |   opc             0x00   0x00
  pop0sr         0x3E   0x00   |   pop1sr          0x06   0x00
  pop2sr         0x3E   0x00   |   pop3sr          0x06   0x00

Per port registers
  mcfgr          0x70   0x00   |   misr            0x41   0x00
  mctlr          0x50   0x00   |   crcsr           0x48   0x00
  transs         0x00   0x00   |   rsop_cier       0x26   0x00
  rsop_sisr      0x5F   0x00   |   rsop_bip80r     0x80   0x00
  rsop_bip81r    0xBB   0x00   |   tsop_ctlr       0x00   0x00
  tsop_diagr     0x00   0x00   |   rlop_csr        0x02   0x00
  rlop_ieisr     0x00   0x00   |   rlop_bip8_240r  0x00   0x00
  rlop_bip8_241r 0x00   0x00   |   rlop_bip8_242r  0x00   0x00
  rlop_febe0r    0x00   0x00   |   rlop_febe1r     0x00   0x00
  rlop_febe2r    0x00   0x00   |   tlop_ctlr       0x20   0x00
  tlop_diagr     0x20   0x00   |   tx_k1           0x00   0x00
  tx_k2          0x00   0x00   |   rpop_scr        0x1C   0x00
  rpop_isr       0x00   0x00   |   rpop_ier        0x00   0x00
  rpop_pslr      0xFF   0x00   |   rpop_pbip80r    0x00   0x00
  rpop_pbip81r   0x00   0x00   |   rpop_pfebe0r    0x00   0x00
  rpop_pfebe1r   0x00   0x00   |   rpop_pbip8cr    0x00   0x00
  tpop_cdr       0x00   0x00   |   tpop_pcr        0x00   0x00
  tpop_ap0r      0x00   0x00   |   tpop_ap1r       0x90   0x00
  tpop_pslr      0x13   0x00   |   tpop_psr        0x00   0x00
  racp_csr       0x84   0x00   |   racp_iesr       0x00   0x00
  racp_mhpr      0x00   0x00   |   racp_mhmr       0x00   0x00
  racp_checr     0x00   0x00   |   racp_uhecr      0x00   0x00
  racp_rcc0r     0x00   0x00   |   racp_rcc1r      0x00   0x00
  racp_rcc2r     0x00   0x00   |   racp_cfgr       0xFC   0x00
  tacp_csr       0x04   0x00   |   tacp_iuchpr     0x00   0x00
  tacp_iucpopr   0x6A   0x00   |   tacp_fctlr      0x10   0x00
  tacp_tcc0r     0xB2   0x00   |   tacp_tcc1r      0x63   0x00
  tacp_tcc2r     0x65   0x00   |   tacp_cfgr       0x08   0x00
  rase_ie        0x07   0x00   |   rase_is         0x00   0x00
  rase_cc        0x00   0x00   |   rase_sfap1      0x08   0x00
  rase_sfap2     0x00   0x00   |   rase_sfap3      0x00   0x00
  rase_sfst1     0xFF   0x00   |   rase_sfst2      0xFF   0x00
  rase_sfdt1     0x45   0x00   |   rase_sfdt2      0x42   0x00
  rase_sfct1     0x86   0x00   |   rase_sfct2      0x82   0x00
  rase_rK1       0xFF   0x00   |   rase_rK2        0xFF   0x00
  rase_rS1       0xFF   0x00

APS control register:    0x0051 |   0x0000
```

```
Local bus timeouts detected:       0
Remote bus timeouts detected:      0
UTOPIA bus parity errors detected: 0

DSLAM> show controllers atm 0/2
IF Name: ATM0/2    Chip Base Address: B3809080
Port type: OC3    Port rate: 155000 kbps    Port medium: MM Fiber

Alarms:
Source: ATM0/2 working  Severity: CRITICAL Description: 10   Loss of Signal

                                  local            peer
                                (working)       (protection)
                                 ACTIVE           INACTIVE
                               ---------------   ---------------
Port status                        SECTION LOS     Not available
Loopback                                  None     Not available
Flags                                   0x8300     Not available
TX clock source                network-derived     Not available
Framing mode                            sts-3c     Not available
Cell payload scrambling                    On     Not available
Sts-stream scrambling                      On     Not available
TX Led:                                   Off     Not available
RX Led:                                    On     Not available
TST Led:                                  Off     Not available

OC3 counters:
  cells transmitted                          0                0
  cells received                             0                0
  cells sent to peer                         0                0
  cells received from peer                   0                0
  section BIP-8 errors                       0                0
  line BIP-8 errors                          0                0
  path BIP-8 errors                          0                0
  OOCD errors (not supported)                0                0
  line FEBE errors                           0                0
  path FEBE errors                           0                0
  correctable HEC errors                     0                0
  uncorrectable HEC errors                   0                0

OC3 errored seconds:
  section BIP-8                              0                0
  line BIP-8                                 0                0
  path BIP-8                                 0                0
  OOCD (not supported)                       0                0
  line FEBE                                  0                0
  path FEBE                                  0                0
  correctable HEC                            0                0
  uncorrectable HEC                          0                0

OC3 error-free secs:
  section BIP-8                              0                0
  line BIP-8                                 0                0
  path BIP-8                                 0                0
  OOCD (not supported)                       0                0
  line FEBE                                  0                0
  path FEBE                                  0                0
  correctable HEC                            0                0
  uncorrectable HEC                          0                0
```

```
                 local   peer                       local   peer
                 -----   ----                       -----   ----
Per chip registers
  mr             0x61    0x00   |   mmc             0x61    0x00
  mcmr           0x67    0x00   |   cscsr           0x67    0x00
  ictl           0x5F    0x00   |   opc             0x00    0x00
  pop0sr         0x3E    0x00   |   pop1sr          0x06    0x00
  pop2sr         0x3E    0x00   |   pop3sr          0x06    0x00

Per port registers
  mcfgr          0x70    0x00   |   misr            0x00    0x00
  mctlr          0x50    0x00   |   crcsr           0x48    0x00
  transs         0x00    0x00   |   rsop_cier       0x26    0x00
  rsop_sisr      0x77    0x00   |   rsop_bip80r     0x80    0x00
  rsop_bip81r    0xBB    0x00   |   tsop_ctlr       0x00    0x00
  tsop_diagr     0x00    0x00   |   rlop_csr        0x02    0x00
  rlop_ieisr     0x00    0x00   |   rlop_bip8_240r  0x00    0x00
  rlop_bip8_241r 0x00    0x00   |   rlop_bip8_242r  0x00    0x00
  rlop_febe0r    0x00    0x00   |   rlop_febe1r     0x00    0x00
  rlop_febe2r    0x00    0x00   |   tlop_ctlr       0x20    0x00
  tlop_diagr     0x20    0x00   |   tx_k1           0x00    0x00
  tx_k2          0x00    0x00   |   rpop_scr        0x1C    0x00
  rpop_isr       0x00    0x00   |   rpop_ier        0x00    0x00
  rpop_pslr      0xFF    0x00   |   rpop_pbip80r    0x00    0x00
  rpop_pbip81r   0x00    0x00   |   rpop_pfebe0r    0x00    0x00
  rpop_pfebe1r   0x00    0x00   |   rpop_pbip8cr    0x00    0x00
  tpop_cdr       0x00    0x00   |   tpop_pcr        0x00    0x00
  tpop_ap0r      0x00    0x00   |   tpop_ap1r       0x90    0x00
  tpop_pslr      0x13    0x00   |   tpop_psr        0x00    0x00
  racp_csr       0x84    0x00   |   racp_iesr       0x00    0x00
  racp_mhpr      0x00    0x00   |   racp_mhmr       0x00    0x00
  racp_checr     0x00    0x00   |   racp_uhecr      0x00    0x00
  racp_rcc0r     0x00    0x00   |   racp_rcc1r      0x00    0x00
  racp_rcc2r     0x00    0x00   |   racp_cfgr       0xFC    0x00
  tacp_csr       0x04    0x00   |   tacp_iuchpr     0x00    0x00
  tacp_iucpopr   0x6A    0x00   |   tacp_fctlr      0x00    0x00
  tacp_tcc0r     0x00    0x00   |   tacp_tcc1r      0x00    0x00
  tacp_tcc2r     0x00    0x00   |   tacp_cfgr       0x08    0x00
  rase_ie        0x07    0x00   |   rase_is         0x00    0x00
  rase_cc        0x00    0x00   |   rase_sfap1      0x08    0x00
  rase_sfap2     0x00    0x00   |   rase_sfap3      0x00    0x00
  rase_sfst1     0xFF    0x00   |   rase_sfst2      0xFF    0x00
  rase_sfdt1     0x45    0x00   |   rase_sfdt2      0x42    0x00
  rase_sfct1     0x86    0x00   |   rase_sfct2      0x82    0x00
  rase_rK1       0xFF    0x00   |   rase_rK2        0xFF    0x00
  rase_rS1       0xFF    0x00

APS control register:    0x0051 |   0x0000

Local bus timeouts detected:       0
Remote bus timeouts detected:      0
UTOPIA bus parity errors detected: 0
```

show dsl interface

To display DSL and ATM status for a port, use the **show dsl interface** command.

show dsl interface [atm | idsl] *slot#/port#*

Syntax Description

slot#/port#	The slot number and port number for the port whose status you want to display. The slot range is 1 to 34. The port range is 1 to 8. (These are maximum ranges; your card might have fewer than 8 ports and your chassis might have fewer than 34 slots. The Cisco 6160 has 32 *x*DSL line card slots. The Cisco 6260 has 30 *x*DSL line cards slots. The Cisco 6015 has 6 *x*DSL line card slots.)

Defaults

There is no default value for this command.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.2(10)DA	The Power Management Additional Margin parameter was added.

Usage Guidelines

Use this command to display line status, loopback status, DSL profile assignment, DSL profile parameters (configured and actual values), alarm status, DSL statistics, and ATM statistics for a port. Table 6-7 describes the fields shown in the **show dsl interface atm** *slot#/port#* for DMT output display.

Table 6-7 show dsl interface Field Descriptions for DMT

Field	Description
Port status:	Heading for the section that displays the general port status.
Subscriber Name:	This output displays the user-defined name of the port or the subscriber (optional).
Circuit ID:	This output displays the user-defined identification field (optional).
IOS admin:	This output displays whether the administrative status of the port is UP or DOWN (**shut**, **no shut**).
oper:	This output displays whether the port is operationally UP or DOWN. The port has to be trained or in loopback for this field to read UP; otherwise it displays DOWN.
Card status:	This output displays the card in the slot if it is present, running, and matches the card type provisioned for the slot; otherwise it displays the status of the card (missing, loading, or specific line card type).

Table 6-7 show dsl interface Field Descriptions for DMT (continued)

Field	Description
Last Change:	This output displays the last time the “oper” or “IOS admin” field changed.
No. of changes:	This output displays the number of operational changes made since card initialization. The only way to clear this field is to pull the card.
Line Status:	This output displays the current operational status of the port (for example, TRAINED, TRAINING, NO CPE DETECTED, LOADING, NOT IN SERVICE, WIDEBAND SIGNAL, DIGITAL LOOPBACK).
Test Mode:	This output displays any current test in progress.
Test Type:	If a test is running or has just completed, this output displays the type of test in progress or just completed (for example, DIGITAL BERT LOOPBACK). This display always appears in the **show dsl interface atm** command for the shdsl and sdsl.
Test Status:	If a test is running or has just completed, this output displays the status of the test. (TEST IN PROGRESS,TEST COMPLETED, TEST WAS ABORTED, NONE)
Test Result:	The first time you use the **show dsl interface** command after a test has been run on the port, the “Test Result” output is available (for example, Error during BERT, Upstream run time (secs), Upstream errors).
ADSL Chipset Self-Test:	This output displays the status of an ADSL chipset self-test. (RUNNING, PASSED, FAILED, NONE)
CO Modem Firmware Version:	This output displays the firmware version that is currently loaded on the DSL line card after the card initializes.
Configured:	Heading for the section that displays information about the profile that is associated with the port specified.
DMT Profile Name:	This output displays the user defined profile name that is assigned to the specific port or subscriber.
Link Traps Enabled:	This output displays whether link traps are enabled or disabled. The default profile does not enable link traps (NO, YES).
Alarms Enabled:	This output displays whether alarms are enabled or disabled. The default profile does not enable the alarms set (NO,YES).
ATM Payload Scrambling:	This output displays whether ATM payload scrambling is enabled or disabled. The default profile enables ATM payload scrambling (Enabled, Disabled). The ATM payload scrambling setting must match the setting on the CPE. This output does not appear for the **show dsl interface idsl** command.
DMT profile parameters	The parameters that display here are identical to the output that displays for the **show dsl profile** command. They are explained in Table 6-12 on page 6-48.

Table 6-7 show dsl interface Field Descriptions for DMT (continued)

Field	Description
Status:	If interprocess communications (IPC) between the NI-2 and line card go down, the line card status fields do not display. If IPC remains down, the **show dsl interface** command becomes unavailable.
Bitrates: Interleave Path: downstream: upstream:	If the port is configured for interleave path, this output displays the actual bitrates of the line; otherwise it displays zero in both fields.
Bitrates: Fast Path: downstream: upstream:	If the port is configured for fast path, this output displays the actual bitrates of the line; otherwise it displays zero in both fields.
Margin: downstream: upstream:	This output displays the actual signal to noise margin at the time you entered the command. The margin should be equal to or higher than the margin configured for the line.
Attenuation: downstream: upstream:	This output displays the actual signal attenuation at the time you entered the command.
Interleave Delay: downstream: upstream:	If the port is configured for interleave path, this output should be equal to or less than your configured interleave delay value. The default is 16 milliseconds.
Transmit Power: downstream: upstream:	This output displays the actual transmit power at the time you entered the command.
Check Bytes (FEC): Interleave Path: downstream: upstream:	If the port is configured for interleave path, this output displays the actual number of check bytes that are configured for the line; otherwise it displays zero in both fields. Higher values increase noise immunity on the DSL link, but they also increase latency. The output might be less than the number configured, depending on the requested line rate and the errors detected.
Check Bytes (FEC): Fast Path: downstream: upstream:	If the port is configured for fast path, this output displays the actual number of check bytes that are configured for the line; otherwise it displays zero in both fields. Higher values increase noise immunity on the DSL link, but they also increase latency. The output might sbe less than the number configured, depending on the requested line rate and the errors detected.
R-S Codeword Size: downstream: upstream:	This output displays the Reed-Solomon codeword size being used. Higher values increase noise immunity on the DSL link, but they also increase latency.
Trellis Coding:	This output displays whether trellis coding is in use on the port.
Overhead Framing:	This output displays the overhead framing mode that is negotiated between the DSLAM and CPE.
Line Fault:	If alarms are enabled and a line or CPE are disconnected, an alarm displays in this output.
Operating Mode:	This field shows either the negotiated operating mode if configured to “auto” or the mode configured (for example, modes G.992.1 or ANSI T1.413).
Line Type:	This output displays either interleave path or fast path, depending on how the port is configured

Table 6-7 show dsl interface Field Descriptions for DMT (continued)

Field	Description
Alarms: status:	If the profile enables the alarms, this output displays any current alarms.
ATM Statistics:	Heading for the section that displays all current counter information for layer 2 (ATM).
Interleaved-Path Counter: Cells: downstream: upstream:	If the port is configured for interleave path, this output displays the actual number of cells sent and received; otherwise it displays zero in both fields.
Interleaved-Path Counter: HEC errors: downstream: upstream:	If the port is configured for interleave path, this output displays the actual number of HEC errors detected; otherwise it displays zero in both fields.
Interleaved-Path Counter: LOCD events: near end: far end:	If the port is configured for interleave path, this output displays the actual number of LOCD events detected; otherwise it displays zero in both fields.
Interleaved-Path Counter: LOCD events before 1st synch: near end:	If the port is configured for interleave path, this output displays the actual number of LOCD events that are detected before the line successfully trained; otherwise it displays zero in both fields. This field is valid only for the 4xflexi dsl line card.
Fast-Path Counters: Cells: downstream: upstream:	If the port is configured for fast path, this output displays the actual number of cells sent and received; otherwise it displays zero in both fields.
Fast-Path Counters: HEC errors: downstream: upstream:	If the port is configured for fast path, this output displays the actual number of HEC errors detected; otherwise it displays zero in both fields.
Fast-Path Counters: LOCD events: near end: far end:	If the port is configured for fast path, this output displays the actual number of LOCD events detected; otherwise it displays zero in both fields.
DSL Statistics:	Heading for the section that displays all current counter information for layer 1.
Init Events:	This output displays the number of initialization attempts for this port.
Far End LPR Events:	This output displays the number of failures caused by a CPE power loss.
Transmitted Superframes: near end: far end:	This output displays the number of superframes sent; near end is the number sent by the DSLAM port, and far end is the number sent and reported by the CPE. With some CPEs, far end sent and received displays zero or not available due to interoperability issues. A superframe is a synchronization boundary that represents 68 x 4 kHz DMT data frames.

Table 6-7 show dsl interface Field Descriptions for DMT (continued)

Field	Description
Received Superframes: near end: far end:	This output displays the number of superframes received; near end is the number received by the port, and far end is the number received and reported by the CPE. With some CPEs, far end sent and received displays zero or not available due to interoperability issues. A superframe is a synchronization boundary that represents 68 x 4 kHz DMT data frames.
Corrected Superframes: near end: far end:	This output displays the number of superframes corrected; near end is the number corrected by the DSLAM, and far end is the number corrected by the CPE. With some CPEs, far end sent and received displays zero or not available due to interoperability issues. A superframe is a synchronization boundary that represents 68 x 4 kHz DMT data frames.
Uncorrected Superframes: near end: far end:	This output displays the number of superframes unable to be corrected; near end is the number unable to be corrected by the DSLAM, and far end is the number unable to be corrected by the CPE. With some CPEs, far end sent and received displays zero or not available due to interoperability issues. A superframe is a synchronization boundary that represents 68 x 4 kHz DMT data frames.
LOS Events: near end: far end:	This output displays the number of LOS events; near end is the number of times this has been detected by the port, and far end is the number of times this has been detected by the CPE.
LOF/RFI Events: near end: far end:	This output displays the number of LOF/RFI events; near end is the number of times this has been detected by the port, and far end is the number of times this has been detected by the CPE.
ES Events: near end: far end:	This output displays the number of ES events; near end is the number of times this has been detected by the port, and far end is the number of times this has been detected by the CPE.
CPE Info:	Heading of the section that displays CPE information.
Version Number:	This output displays a unique number defined per CPE vendor and model.
Vendor ID:	This output displays a unique number defined per CPE vendor and model.

Table 6-8 describes the fields shown in the **show dsl interface atm** *slot#/port#* for SHDSL output display.

Table 6-8 show dsl interface Field Descriptions for SHDSL

Field	Description
Port status:	Heading for the section that displays the general port status.
Subscriber Name:	This output displays the user defined name of the port or the subscriber (optional).
Circuit ID:	This output displays the user defined identification field (optional).

Table 6-8 show dsl interface Field Descriptions for SHDSL (continued)

Field	Description
IOS admin:	This output displays whether the administrative status of the port is UP or DOWN (**shut**, **no shut**).
oper:	This output displays whether the port is operationally UP or DOWN. The port must be trained or in loopback for this field to read UP; otherwise it displays DOWN.
Card status:	This output displays the card in the slot if it is present, running, and matches the card type provisioned for the slot; otherwise it displays the status of the card (missing, loading, or specific line card type).
Last Change:	This output displays the last time the "oper" or "IOS admin" field changed.
No. of changes:	This output displays the number of operational changes made since card initialization, the only way to clear this field is to pull the card.
Line Status:	This output displays the current operational status of the port (for example, TRAINED, TRAINING, NO CPE DETECTED, LOADING, NOT IN SERVICE, WIDEBAND SIGNAL, DIGITAL LOOPBACK).
Test Mode:	This output displays any current test in progress.
Test Type:	If a test is running or has just been completed, this output displays the type of test in progress or just completed (for example, DIGITAL BERT LOOPBACK). This display always appears in the **show dsl interface atm** command for shdsl and sdsl.
Test Status:	If a test is running or has just been completed, this output displays the status of the test. (TEST IN PROGRESS,TEST COMPLETED, TEST WAS ABORTED, NONE)
Test Result:	The first time you use the **show dsl interface** command after a test is run on the port, the "Test Result" output is available (for example, Error during BERT, Upstream run time (secs), Upstream errors).
Configured:	Heading for the section that displays information about the profile that is associated with the port specified.
SHDSL Profile Name:	This output displays the user defined profile name that is assigned to the specific port or subscriber.
Link Traps Enabled:	This output displays whether link traps are enabled or disabled. The default profile does not enable link traps (NO, YES).
Alarms Enabled:	This output displays whether alarms are enabled or disabled. The default profile does not enable the alarms set (NO, YES).
ATM Payload Scrambling:	This output displays whether ATM payload scrambling is enabled or disabled. The default profile enables ATM payload scrambling (Enabled, Disabled). The ATM payload scrambling setting must match the setting on the CPE. This output does not appear for the **show dsl interface idsl** command.
[CAP, DMT, IDSL, SDSL, SHDSL] profile parameters	The parameters that display here are identical to the output that displays for the **show dsl profile** command. These parameters are explained in Table 6-12 on page 6-48.

Table 6-8 show dsl interface Field Descriptions for SHDSL (continued)

Field	Description
DSP/Framer Version: Hardware Ver:	This output displays the hardware version that is currently loaded on the DSL line card after the card initializes.
DSP/Framer Version: Firmware Ver:	This output displays the firmware version that is currently loaded on the DSL line card after the card initializes.
Status: (This status output is valid for SHDSL)	If interprocess communications (IPC) between the NI-2 and line card goes down, the line card status fields do not display. If IPC remains down, the **show dsl interface** command becomes unavailable.
Actual bitrates:	This output displays the actual data rate on the port.
Receiver gain: near end:	This output displays the reporting by the DSLAM of the amount of gain required to receive the signal. This number varies depending on signal attenuation and the transmit power of the CPE.
Transmit power: near end:	This output displays the amount of power that the DSLAM is transmitting out the specific port.
Run-time receiver SNR near end:	This output displays the real-time signal to noise ratio for the signal that the port receives.
SNR Margin: near end:	This output displays the actual signal to noise margin at the time you enter the command. The margin should be equal to or higher than the margin configured for the line.
Attenuation: near end:	This output displays the actual signal attenuation at the time you enter the command.
Alarms: Status:	If the profile enables the alarms, this output displays any current alarms.
Alarms: Defects:	If the profile enables the alarms, this output displays any alarm defects.
Alarms: status:	If the profile enables the alarms, this output displays any current alarms.
ATM Statistics:	Heading for the section that displays all current counter information for Layer 2 (ATM).
ATM Statistics: Cells: downstream: upstream:	This output displays the actual number of cells sent and received.
ATM Statistics: HEC errors: upstream:	This output displays the actual number of header error control (HEC) errors detected.
DSL Statistics:	Heading for the section that displays all current counter information for layer 1.
Init Events: near end:	This output displays the number of initialization attempts for this port.

Table 6-8 show dsl interface Field Descriptions for SHDSL (continued)

Field	Description
LOS Events: near end:	This output displays the number of loss of signal (LOS) events that the port detects.
LOSQ Events: near end:	This output displays the number of loss of signal quality (LOSQ) events that the port detects.
SES Events: near end:	This output displays the number of severely errored seconds (SES) that the port detects.
CV Events: near end:	This output displays the number of coding violations (CV) that the port detects.
ES Events: near end:	This output displays the number of errored seconds (ES) that the port detects.
UAS Events: near end:	This output displays the number of unavailable seconds (UAS) that the port detects.
Unavailable Resources: near end:	This output displays the counter for upstream cell loss between the line card and the NI-2.

Table 6-9 describes the fields shown in the **show dsl interface atm** *slot#/port#* for SDSL output display.

Table 6-9 show dsl interface Field Descriptions for SDSL

Field	Description
Port status:	Heading for the section that displays the general port status.
Subscriber Name:	This output displays the user-defined name of the port or the subscriber (optional).
Circuit ID:	This output displays the user-defined identification field (optional).
IOS admin:	This output displays whether the administrative status of the port is UP or DOWN (**shut**, **no shut**).
oper:	This output displays whether the port is operationally UP or DOWN. The port has to be trained or in loopback for this field to read UP; otherwise it displays DOWN.
Card status:	This output displays the card in the slot if it is present, running, and matches the card type provisioned for the slot; otherwise it displays the status of the card (missing, loading, or specific line card type).
Last Change:	This output displays the last time the “oper” or “IOS admin” field changed.
No. of changes:	This output displays the number of operational changes made since card initialization; the only way to clear this field is to pull the card.
Line Status:	This output displays the current operational status of the port (for example, TRAINED, TRAINING, NO CPE DETECTED, LOADING, NOT IN SERVICE, WIDEBAND SIGNAL, DIGITAL LOOPBACK).

Table 6-9 show dsl interface Field Descriptions for SDSL (continued)

Field	Description
Test Mode:	This output displays any current test in progress.
Test Type:	If a test is running or has just completed, this output displays the type of test in progress or just completed (for example, DIGITAL BERT LOOPBACK). This display always appears in the **show dsl interface atm** command for shdsl and sdsl.
Test Status:	If a test is running or has just completed, this output displays the status of the test. (TEST IN PROGRESS, TEST COMPLETED, TEST WAS ABORTED, NONE).
Test Result:	The first time you use the **show dsl interface** command after a test has run on the port, the "Test Result" output is available (for example, Error during BERT, Upstream run time (secs), Upstream errors).
Configured:	Heading for the section that displays information about the profile that is associated with the port specified.
SDSL Profile Name:	This output displays the user defined profile name that is assigned to the specific port or subscriber.
Link Traps Enabled:	This output displays whether link traps are enabled or disabled. The default profile does not enable link traps (NO, YES).
Alarms Enabled:	This output displays whether alarms are enabled or disabled. The default profile does not enable the alarms set (NO, YES).
ATM Payload Scrambling:	This output displays whether ATM payload scrambling is enabled or disabled. The default profile enables ATM payload scrambling (Enabled, Disabled). The ATM payload scrambling setting must match the setting on the CPE. This output does not appear for the **show dsl interface idsl** command.
[CAP, DMT, IDSL, SDSL, SHDSL] profile parameters	The parameters that display here are identical to the output that displays for the **show dsl profile** command and are explained in Table 6-12 on page 6-48.
Default configurations: Transmit Power: 0 dB	This output displays that the default configuration for transmit power is 0 dB.
Default configurations: Retrain level: 20 dB	This output indicates that when the signal to noise ratio reaches 20 dB, the line is dropped and then retrains.
Default configurations: Retrain Timeout: 180 secs	This output displays that the default configuration for the retrain timeout is 180 seconds. If the training process takes 180 seconds, the process stops and starts over.
DSP/Framer Version: Hardware Ver:	This output specifies the hardware version that is currently loaded on the DSL line card after the card initializes.
DSP/Framer Version: Firmware Ver:	This output specifies the firmware version that is currently loaded on the DSL line card after the card initializes.

Table 6-9 show dsl interface Field Descriptions for SDSL (continued)

Field	Description
Status: (This status output is valid for SDSL)	If interprocess communications (IPC) between the NI-2 and line card goes down, the line card status fields does not display. If IPC remains down, the **show dsl interface** command becomes unavailable.
Actual bitrates:	This output displays the actual data rate on the port.
Receiver gain: near end:	This output displays the reporting by the DSLAM of the amount of gain required to receive the signal. This number varies depending on signal attenuation and the transmit power of the CPE.
Transmit power: near end:	This output displays the amount of power that the DSLAM is transmitting out of the specific port.
Run-time receiver SNR: near end:	This output displays the real-time signal to noise margin for the signal that the port receives.
Alarms: status:	If the profile enables the alarms, this output displays any current alarms.
ATM Statistics:	Heading for the section that displays all current counter information for Layer 2 (ATM).
ATM Statistics: Cells: downstream: upstream:	This output displays the actual number of cells sent and received.
ATM Statistics: HEC errors: upstream:	This output displays the actual number of header error control (HEC) errors detected.
DSL Statistics:	Heading for the section that displays all current counter information for layer 1.
Init Events: near end:	This output displays the number of initialization attempts for this port.
LOS Events: near end:	This output displays the number of loss of signal (LOS) events that the port detects.

Table 6-10 describes the fields shown in the **show dsl interface atm** *slot#/port#* for CAP output display.

Table 6-10 show dsl interface Field Descriptions for CAP

Field	Description
Port status:	Heading for the section that displays the general port status.
Subscriber Name:	This output displays the user defined name of the port or the subscriber (optional).
Circuit ID:	This output displays the user defined identification field (optional).
IOS admin:	This output displays whether the administrative status of the port is UP or DOWN (**shut**, **no shut**).
oper:	This output displays whether the port is operationally UP or DOWN. The port has to be trained or in loopback for this field to read UP; otherwise it displays DOWN.
Card status:	This output displays the card in the slot if it is present, running, and matches the card type provisioned for the slot; otherwise it displays the status of the card (missing, loading, or specific line card type).
Last Change:	This output displays the last time the “oper” or “IOS admin” field changed.
No. of changes:	This output displays the number of operational changes made since card initialization; the only way to clear this field is to pull the card.
Line Status:	This output displays the current operational status of the port (for example, TRAINED, TRAINING, NO CPE DETECTED, LOADING, NOT IN SERVICE, WIDEBAND SIGNAL, DIGITAL LOOPBACK).
Test Mode:	This output displays any current test in progress.
Test Type:	If a test is running or has just completed, this output displays the type of test in progress or just completed (for example, DIGITAL BERT LOOPBACK). This display always appears in the **show dsl interface atm** command for shdsl.
Test Status:	If a test is running or has just been completed, this output displays the status of the test. (TEST IN PROGRESS,TEST COMPLETED, TEST WAS ABORTED, NONE.)
Test Result:	The first time you use the **show dsl interface** command after a test has run on the port, the “Test Result” output is available (for example, Error during BERT, Upstream run time (secs), Upstream errors).
ADSL Chipset Self-Test:	This output displays the status of an ADSL chipset self-test (RUNNING, PASSED, FAILED, NONE).
CO Modem Firmware Version:	Heading for the section that displays the CO modem firmware version.
CO Modem Firmware Version: DSP Version:	This output displays the DSP version that is currently loaded on the dsl line card after the card initializes.
CO Modem Firmware Version: DSP Firmware Release:	This output displays the DSP firmware version that is currently loaded on the dsl line card after the card initializes.

Table 6-10 show dsl interface Field Descriptions for CAP (continued)

Field	Description
CO Modem Firmware Version: CO Protocol Version:	This output displays the CO protocol version that is currently loaded on the DSL line card after the card initializes.
Configured:	Heading for the section that displays information about the profile that is associated with the port specified.
CAP Profile Name:	This output displays the user defined profile name that is assigned to the specific port or subscriber.
Link Traps Enabled:	This output displays whether link traps are enabled or disabled. The default profile does not enable link traps (NO, YES).
Alarms Enabled:	This output displays whether alarms are enabled or disabled. The default profile does not enable the alarms set (NO, YES).
ATM Payload Scrambling:	This output displays whether ATM payload scrambling is enabled or disabled. The default profile enables ATM payload scrambling (Enabled, Disabled). The ATM payload scrambling setting must match the setting on the CPE. This output does not appear for the **show dsl interface idsl** command.
[CAP, DMT, IDSL, SDSL, SHDSL] profile parameters	The parameters that display here are identical to the output that displays for the **show dsl profile** command and are explained in Table 6-12 on page 6-48.
Status: (This status output is valid for CAP)	If interprocess communications (IPC) between the NI-2 and line card goes down, the line card status fields do not display. If IPC remains down, the **show dsl interface** command becomes unavailable.
Bitrates: downstream: upstream:	This output displays the actual downstream and upstream data rate on the port.
Constellation: downstream: upstream:	This output displays the actual constellation downstream and upstream on the port.
Baud Rate: downstream: upstream:	This output displays the actual downstream and upstream baud rate on the port.
Signal Quality co: cpe:	This output displays the signal quality for the signal that the port sends and receives.
Receiver Gain: co: cpe:	This output displays the reporting by the DSLAM of the amount of gain required to receive the signal, and the number varies depending on attenuation and CPE transmit power.
Transmit Power: co: cpe:	This output displays the amount of power the DSLAM is transmitting and receiving out the specific port.
SNR co:	This output displays the signal to noise ratio for the signal that the port receives.
Margin: upstream:	This output displays the signal to noise margin for the signal that the port receives.

Table 6-10 show dsl interface Field Descriptions for CAP (continued)

Field	Description
Alarms: status:	If the profile enables the alarms, this output displays any current alarms.
ATM Statistics:	Heading for the section that displays all current counter information for layer 2(ATM).
ATM Statistics: Cells: downstream: upstream:	This output displays the actual number of cells sent and received.
ATM Statistics: HEC errors: upstream:	This output displays the actual number of header error control (HEC) errors detected.
DSL Statistics:	Heading for the section that displays all current counter information for layer 1.
Init Events:	This output displays the number of initialization attempts for this port.
CPE Info:	Heading of the section that displays CPE information.
Vendor ID:	This output displays a unique number defined per CPE vendor and model.
Product ID:	This output displays a unique number defined per CPE vendor and model.
Protocol:	This output displays the protocol being used by the CPE.
Signature:	This output displays a unique signature defined per CPE vendor and model.

Table 6-11 describes the fields shown in the **show dsl interface atm** *slot#/port#* for IDSL output display.

Table 6-11 show dsl interface Field Descriptions for IDSL

Field	Description
Port status:	Heading for the section that displays the general port status.
Subscriber Name:	This output displays the user-defined name of the port or the subscriber (optional).
Circuit ID:	This output displays the user-defined identification field (optional).
IOS admin:	This output displays whether the administrative status of the port is UP or DOWN (**shut**, **no shut**).
oper:	This output displays whether the port is operationally UP or DOWN. The port has to be trained or in loopback for this field to read UP; otherwise it displays DOWN.
Card status:	This output displays the card in the slot if it is present, running, and matches the card type provisioned for the slot; otherwise it displays the status of the card (missing, loading, or specific line card type).
Last Change:	This output displays the last time the “oper” or “IOS admin” field changed.

Table 6-11 show dsl interface Field Descriptions for IDSL (continued)

Field	Description
No. of changes:	This output displays the number of operational changes made since card initialization; the only way to clear field this field is to pull the card.
Loopback:	This output displays whether loopback is enabled or disabled on the port.
Firmware version:	This output displays the firmware version on the idsl line card.
BERT has not been executed on this interface	This outputs displays whether a BERT test has been executed on the interface.
Configured:	Heading for the section that displays information about the profile associated with the port specified.
Profile Name:	This output displays the user-defined profile name that is assigned to the specific port or subscriber.
Alarms Enabled:	This output displays whether alarms are enabled or disabled. The default profile does not enable the alarms set (NO, YES).
[CAP, DMT, IDSL, SDSL, SHDSL] profile parameters	The parameters that display here are identical to the output that displays for the **show dsl profile** command and are explained in Table 6-12 on page 6-48.
Performance Statistics: (This status output is valid for IDSL)	Heading for the section that displays idsl port status.
Physical Layer Coding violations:	This output displays coding violations that the DSLAM detects at the physical layer.
Physical Layer Errored seconds:	This output displays errored seconds that the DSLAM detects at the physical layer.
Physical Layer Severely errored seconds:	This output displays severely errored seconds that the DSLAM detects at the physical layer.
Physical Layer (far end) Coding violations:	This output displays coding violations detected by the CPE at the physical layer.
Physical Layer (far end) Errored seconds:	This output displays errored seconds detected by the CPE at the physical layer.
Physical Layer (far end) Severely errored seconds:	This output displays severely errored seconds detected by the CPE at the physical layer.
HDLC Layer Coding violations:	This output displays coding violations that the DSLAM detects at the HDLC layer.
HDLC Layer Aborts:	This output displays the number of HDLC aborts detected by the DSLAM.
HDLC Layer Aligns:	This output displays the number of “aligns” or frames received with a number a bits not divisible by 8.

Table 6-11 show dsl interface Field Descriptions for IDSL (continued)

Field	Description
HDLC Layer Shorts:	This output displays the number of "shorts" or frames received that are less than 5 bytes in length.
HDLC Layer Longs:	This output displays the number of "longs" or frames received that are larger than the maximum transmission unit (MTU).
HDLC Layer Discards:	This output displays the number of frames dropped due to an error condition. Error conditions include shorts, longs, and line congestion.
Alarm Status:	If the profile enables the alarms, this output displays any current alarms.

Examples

In this example, the command displays the DSL/DMT and ATM status for slot 1, port 1.

Note The outputs for profile parameters vary (cap, dmt, idsl, sdsl, shdsl), depending on which form of DSL technology your system is using in a particular slot.

```
DSLAM> show dsl interface atm 1/1
Port Status:
    Subscriber Name:          Circuit ID:
    IOS admin: UP     oper: UP     Card status: ATUC-8-DMT-1-H
    Last Change: 00 days, 00 hrs, 13 min, 05 sec No. of changes: 5
    Line Status: TRAINED
    Test Mode: NONE

 ADSL Chipset Self-Test: NONE

 CO Modem Firmware Version: P.70

 Configured:
       DMT Profile Name: default
       Link Traps Enabled: NO
       Alarms Enabled: NO
       ATM Payload Scrambling: Enabled

DMT profile parameters
      Maximum Bitrates:
         Interleave Path:   downstream:   640 kb/s,   upstream:   128 kb/s
         Fast Path:         downstream:     0 kb/s,   upstream:     0 kb/s
      Minimum Bitrates:
         Interleave Path:   downstream:     0 kb/s,   upstream:     0 kb/s
         Fast Path:         downstream:     0 kb/s,   upstream:     0 kb/s
      Margin:               downstream:     6 dB,     upstream:     6 dB
      Interleaving Delay:   downstream: 16000 usecs,  upstream: 16000 usecs
      Check Bytes (FEC):
         Interleave Path:   downstream:    16,        upstream:    16
         Fast Path:         downstream:     0,        upstream:     0
      R-S Codeword Size:    downstream:  auto,        upstream:  auto
      Trellis Coding:         Disabled
      Overhead Framing:       Mode 3
      Operating Mode:         Automatic
      Training Mode:          Quick
      Minrate blocking:       Disabled
```

```
     SNR Monitoring:         Disabled
     Power Management Additional Margin:
               downstream:     2 dB,     upstream:     3 dB

Status:
    Bitrates:
         Interleave Path:   downstream:   640 kb/s,   upstream:   128 kb/s
         Fast Path:         downstream:     0 kb/s,   upstream:     0 kb/s
    Attainable Aggregate
    Bitrates:
                            downstream:  8064 kb/s,   upstream:   800 kb/s
    Margin:                 downstream:    36 dB,     upstream:    35 dB
    Attenuation:            downstream:     1 dB,     upstream:     1 dB
    Interleave Delay:       downstream: 16000 usecs,  upstream: 16000 usecs
    Transmit Power:         downstream:   9.0 dB,        upstream:  11.3 dB
    Check Bytes (FEC):
         Interleave Path:   downstream:    16,        upstream:    16
         Fast Path:         downstream:     0,        upstream:     0
    R-S Codeword Size:      downstream:     1,        upstream:    16
    Trellis Coding:           In Use
    Overhead Framing:         Mode 3
    Line Fault:               NONE
    Operating Mode:           ANSI T1 413 Issue 2
    Line Type:                Interleaved Only

    Alarms:
       status:                NONE

ATM Statistics:
   Interleaved-Path Counters:
      Cells:                downstream:          0     upstream:        172
      HEC errors:           downstream:          0     upstream:          0
      LOCD events:          near end:            0     far end:           0
   Fast-Path Counters:
      Cells:                downstream:          0     upstream:          0
      HEC errors:           downstream:          0     upstream:          0
      LOCD events:          near end:            0     far end:           0

DSL Statistics:
   Init Events:             1
   Far End LPR Events:      0
   Transmitted Superframes: near end:        46476     far end:           0
   Received Superframes:    near end:        46311     far end:           0
   Corrected Superframes:   near end:            0     far end:           0
   Uncorrected Superframes: near end:            5     far end:           0
   LOS Events:              near end:            0     far end:           0
   LOF/RFI Events:          near end:            0     far end:           0
   ES Events:               near end:            1     far end:           0

CPE Info:
   Version Number:            1
   Vendor ID:                 34
```

Related Commands

Command	Description
show dsl status	To display the current status of the DSL subscriber ports on a chassis
dsl-copy-profile	Copies a DSL profile.
dsl-profile	Creates a DSL profile or selects an existing profile for modification.
dsl profile	Attaches a port to a profile.

show dsl profile

To display a specific profile or all existing profiles, use the **show dsl profile** command.

show dsl profile [*profile-name*]

Syntax Description

[*profile-name*]	(Optional.) The name of the profile you want to display.

Defaults

If you omit the *profile-name* argument, this command displays profile information for all existing profiles.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

This command displays port configuration settings for selected profiles. Table 6-12 describes the fields shown in the display.

Table 6-12 show dsl profile default Field Descriptions

Field	Description
dsl profile default:	Heading for the section that displays the dsl profile parameters. The "default" in this field name of the profile can be given as a command line option. All profiles will be shown by the **show dsl profile** command; to display profiles individually, add the specific profile name to the command.
Link Traps Enabled:	This output displays whether link traps are enabled or disabled. The default profile does not enable link traps (NO, YES).
Alarms Enabled:	This output displays whether alarms are enabled or disabled. The default profile does not enable the alarms set (NO, YES).
ATM payload Scrambling:	This output displays whether ATM payload scrambling is enabled or disabled. The default profile enables ATM payload scrambling (Enabled, Disabled). The ATM payload scrambling setting must match the setting on the CPE.
DMT profile parameters	Heading for the section that displays the DMT profile parameters.
Maximum Bitrates: Interleave Path: downstream: upstream:	If the port is configured for interleave path, this output displays the configured maximum bitrates both downstream and upstream for the line; otherwise it displays zero in both fields.

Table 6-12 show dsl profile default Field Descriptions (continued)

Field	Description
Maximum Bitrates: Fast Path: downstream: upstream:	If the port is configured for fast path, this output displays the configured maximum bitrates both downstream and upstream for the line; otherwise it displays zero in both fields.
Minimum Bitrates: Interleave Path: downstream: upstream:	If the port is configured for interleave path, this output displays the configured minimum bitrates both downstream and upstream for the line; otherwise it displays zero in both fields. If the data rate drops below this threshold, an alarm will be sent.
Minimum Bitrates: Fast Path: downstream: upstream:	If the port is configured for fast path, this output displays the configured minimum bitrates both downstream and upstream for the line; otherwise it displays zero in both fields. If the data rate drops below this threshold, an alarm will be sent.
Margin: downstream: upstream:	This output displays the user determined minimum allowed signal to noise margin for the port.
Interleaving Delay: downstream: upstream:	This output displays the configured interleave delay value. The default is 16 milliseconds. If no errors are being reported, you can reduce this number for less latency.
Check Bytes (FEC): Interleave Path: downstream: upstream:	If the port is configured for interleave path, this output displays the configured number of check bytes for the line; otherwise it displays zero in both fields.
Check Bytes (FEC): Fast Path: downstream: upstream:	If the port is configured for fast path, this output displays the configured number of check bytes for the line; otherwise it displays zero in both fields.
R-S Codeword Size: downstream: upstream:	This output displays the Reed-Solomon codeword size that is configured on the port. The default is auto which allows the algorithm to optimize performance.
Trellis Coding:	This output displays whether trellis coding is enabled on the port (Enabled, Disabled).
Overhead Framing:	This output displays the overhead framing mode that is configured for the port. The default is Mode 3, which optimizes performance (Mode 0, Mode 1, Mode 2, Mode 3).
Operating Mode:	This output displays the configured operating mode on the port (for example G.992.1 or ANSI T1.413).
Training Mode:	This output displays the training mode that is configured on the port. The default is quick.
Minrate blocking:	Displays minimum rate allowed to train. If the line cannot meet this rate, it does not train.
SNR Monitoring:	If SNR monitoring is enabled, this output displays the minimum margin and interval value for both upstream and downstream. The default is Disabled (Enabled, Disabled).
Power Management Additional Margin:	Displays the configured values in decibels for both downstream and upstream.

Table 6-12 show dsl profile default Field Descriptions (continued)

Field	Description
SDSL profile parameters	Heading for the section that displays the SDSL profile parameters.
Maximum Bitrates:	This output displays the configured maximum bitrates, both downstream and upstream, for the line.
SHDSL profile parameters	Heading for the section that displays the SHDSL profile parameters.
Maximum Bitrates:	This output displays the configured maximum bitrates, both downstream and upstream, for the line.
SNR margin threshold:	This output displays the configured threshold. If the noise margin cannot be maintained at the threshold value, an alarm is sent. The default is 3 dB.
SNR margin target:	This output displays the configured margin the modem must maintain relative to a BER of 10^{-7}. The default is 0 dB
SNR margin min:	This output displays the configured minimum noise margin the modem must achieve to trainup. The default is 0 dB.
Masktype:	This output displays the masktype: Symmetric (only).
Annex:	This output displays the configured setting; the default is A (North America). Annex B (Europe) is the other option.
Rate Mode:	This output displays the rate mode (fixed).
CAP profile parameters	Heading for the section that displays the CAP profile parameters.
Maximum Bitrates: downstream: upstream:	This output displays the configured maximum bitrates, both downstream and upstream, for the line.
Minimum Bitrates: downstream: upstream:	This output displays the configured minimum bitrates, both downstream and upstream, for the line. If the data rate drops below this threshold, an alarm is sent.
Margin downstream: upstream:	This output displays the user-determined minimum allowed signal to noise margin for the port.
PSDM: downstream: upstream:	This output displays the actual power spectral density mask on the port.
Interleaving Delay:	This output displays the configured interleave delay setting (long, short, none). The default setting is long. Setting the interleave delay to none disables the Reed-Solomon algorithm.
136K Baud DS Rates:	This output displays whether the line is allowed to train at this low rate (Enabled, Disabled). You can set this rate for both downstream and upstream rates.
68K BAUD US Rates:	This output displays whether the line is allowed to train at this low rate (Enabled, Disabled). You can set this rate for both downstream and upstream rates.
17K Baud US Rates:	This output displays whether the line is allowed to train at this low rate (Enabled, Disabled). You can set this rate for both downstream and upstream rates.

Table 6-12 show dsl profile default Field Descriptions (continued)

Field	Description
CPE Signature:	This output displays a number uniquely defined per CPE vendor and model.
IDSL profile parameters	Heading for the section that displays the IDSL profile parameters.
Bitrate:	This output displays the bit rate that is configured for the port; options include 144, 128, 64, and 56. The default is 128.
Encapsulation:	This output displays the type of encapsulation that the specific port uses. The default is llc-ppp; other options include cisco-ppp, frame-relay, and mux-ppp.
Frame Relay Parameters: UPC intent:	If the port was configured for frame relay encapsulation, this output displays the usage parameter control (UPC) setting (PASS, TAG, DROP). This setting is used for traffic policing.
Frame Relay Parameters: Bc default:	If the port was configured for frame relay encapsulation, this output displays the committed burst size to be used for ABR/UBR soft virtual channels that terminate on an interface. The range is 0 through 32768. The default is set at the maximum, 32768.
Frame Relay Parameters: LMI type:	If the port was configured for frame relay encapsulation, this output displays the local management interface (LMI) type (ansi, cisco, q933a, none). The default is cisco.
Frame Relay Parameters: lmi-n392dce:	If the port was configured for frame relay encapsulation, this output displays the frame relay data communications equipment (DCE) error threshold for the port. The range is 1 through 10. The default is set at 2.
Frame Relay Parameters: lmi-n393dce:	If the port was configured for frame relay encapsulation, this output displays the frame relay DCE monitored events count. The range is 1 through 10. The default is set at 2.
Frame Relay Parameters: lmi-t392dce:	If the port was configured for frame relay encapsulations, this output displays the frame relay DCE polling verification timer. The range is 5 through 30 seconds. The default is set at 15 seconds.

Examples

In this example, the command displays the profile default:

```
DSLAM> show dsl profile default
dsl profile default:
    Link Traps Enabled: NO
    Alarms Enabled: NO
    ATM Payload Scrambling: Enabled

    DMT profile parameters
          Maximum Bitrates:
             Interleave Path:   downstream:     0 kb/s,   upstream:     0 kb/s
             Fast Path:         downstream:  8064 kb/s,   upstream:  1024 kb/s
          Minimum Bitrates:
             Interleave Path:   downstream:     0 kb/s,   upstream:     0 kb/s
             Fast Path:         downstream:     0 kb/s,   upstream:     0 kb/s
          Margin:               downstream:     6 dB,     upstream:     6 dB
          Interleaving Delay:   downstream: 16000 usecs,  upstream: 16000 usecs
          Check Bytes (FEC):
             Interleave Path:   downstream:    16,        upstream:    16
```

```
        Fast Path:         downstream:     0,        upstream:     0
      R-S Codeword Size:   downstream:  auto,        upstream:  auto
      Trellis Coding:        Disabled
      Overhead Framing:      Mode 3
      Operating Mode:        Automatic
      Training Mode:         Quick
      Minrate blocking:      Disabled
      SNR Monitoring:        Disabled
Power Management Additional Margin:
 downstream:     0 dB,     upstream:     0 dB
SDSL profile parameters
    Maximum Bitrates: 784 kbps
SHDSL profile parameters
    Maximum Bitrates: 776 kbps
    SNR margin threshold: 3 dB
    SNR margin target: 0 dB
    SNR margin min: 0 dB
    Masktype: symmetric
    Annex: A
    Rate mode: fixed
CAP profile parameters
    Maximum Bitrates: downstream: 640 kb/s, upstream: 91 kb/s
    Minimum Bitrates: downstream: 0 kb/s, upstream: 0 kb/s
    Margin: downstream: 3 dB, upstream: 6 dB
    PSDM: downstream: -40 dBm/Hz, upstream: -38 dBm/Hz
    Interleaving Delay: Long (Reed-Solomon enabled)
    136K Baud DS Rates: Enabled
    68K Baud US Rates: Disabled
    17K Baud US Rates: Disabled
    CPE Signature: 0
IDSL profile parameters
    Bitrate: 128 kbit/sec
    Encapsulation: llc-ppp
    Frame Relay parameters:
    UPC intent: pass
    Bc default: 32768 bytes
    LMI type: cisco
    lmi-n392dce: 2 events
    lmi-n393dce: 2 events
    lmi-t392dce: 15 seconds
```

Related Commands

Command	Description
dsl-copy-profile	Copies a DSL profile.
dsl-profile	Creates a DSL profile or selects an existing profile for modification.
dsl profile	Attaches a port to a profile.
show running-config	Displays the running configuration for every currently defined profile, including the default.

show dsl status

To display the current status of the DSL subscriber ports on a chassis, use the **show dsl status** exec command.

show dsl status

Syntax Description

The command has no arguments or keywords.

Defaults

If you omit optional arguments, this command displays the status of the DSL subscriber ports for all interface types on a chassis.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

This command displays the following information for each DSL port on a chassis:

- Subtend node ID for the chassis, if any
- Administrative state of the port (up/down)

Note Output items for SDSL ports display one value for both upstream and downstream.

- Operational state of the port (up/down)
- Actual, trained upstream and downstream bit rates for the connection (not configured values)
- Subscriber name associated with the port (truncated at 10 characters)
- Circuit ID associated with the port (truncated at 10 characters)

Examples

In this example, the command displays the status for all of the DSL subscriber ports on a Cisco 6015 chassis:

```
DSLAM> show dsl status

Subtend Node ID: 0

                        DOWNSTREAM   UPSTREAM   SUBSCRIBER     CIRCUIT ID
   NAME   ADMIN/OPER         (Kb)       (Kb)   (truncated)    (truncated)
   ----   ----------     --------   --------   -----------    -----------
 ATM1/1      UP/DOWN            0          0
 ATM1/2      UP/DOWN            0          0
 ATM1/3      UP/DOWN            0          0
 ATM1/4      UP/DOWN            0          0
 ATM1/5      UP/DOWN            0          0
```

```
ATM1/6      UP/DOWN          0          0
ATM1/7      UP/DOWN          0          0
ATM1/8      UP/DOWN          0          0
ATM2/1      UP/DOWN          0          0
ATM2/2      UP/DOWN          0          0
ATM2/3      UP/DOWN          0          0
ATM2/4      UP/DOWN          0          0
ATM2/5      UP/DOWN          0          0
ATM2/6      UP/DOWN          0          0
ATM2/7      UP/DOWN          0          0
ATM2/8      UP/DOWN          0          0
ATM3/1      UP/DOWN          0          0
ATM3/2      UP/DOWN          0          0
ATM3/3      UP/DOWN          0          0
ATM3/4      UP/DOWN          0          0
ATM4/1      UP/DOWN          0          0
ATM4/2      UP/DOWN          0          0
ATM4/3      UP/DOWN          0          0
ATM4/4      UP/DOWN          0          0
ATM5/1      UP/DOWN          0          0
ATM5/2      UP/DOWN          0          0
ATM5/3      UP/DOWN          0          0
ATM5/4      UP/DOWN          0          0
ATM6/1      UP/DOWN          0          0
ATM6/2      UP/DOWN          0          0
ATM6/3      UP/DOWN          0          0
ATM6/4      UP/DOWN          0          0
ATM6/5      UP/DOWN          0          0
ATM6/6      UP/DOWN          0          0
ATM6/7      UP/DOWN          0          0
ATM6/8      UP/DOWN          0          0
```

Related Commands

Command	Description
show dsl interface atm	Displays the line coding status for a port.

show dsl status cap

To troubleshoot CAP ports, use the **show dsl status cap** command.

show dsl status cap

Syntax Description

The command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)DA	This command was modified to provide CAP specific feedback.

Usage Guidelines

Use this command to determine the administrative and operational status of each port. Nothing displays for slots that are empty and unprovisioned. This command also provides information on SNRs, HEC errors, line rates, receiver gain, and detected CAP cards.

Table 6-13 describes the fields shown in the display.

Table 6-13 show dsl status cap Field Descriptions

Field	Description
NAME	This output displays the ATM slot(s) and ports.
ADMIN/OPER	This output displays whether the port is administratively up or down and whether the port is operationally (physically) up or down.
DWNSTRN (Kb)	This output displays the actual downstream data rate on the port.
UPSTRN (Kb)	This output displays the actual upstream data rate on the port.
RCVR GAIN	This output displays the reporting bye the DSLAM of the amount of gain required to receive the signal. The number varies depending on attenuation and CPE transmit power.
TX POWER	This output displays the amount of power the DSLAM is transmitting out the specific port.
RCVR SNR	This output displays the signal to noise ratio of the signal that the port receives.
UPSTRN MARGIN	This output displays the signal to noise margin of the signal that the port receives.
HEC ERROR	This output displays the number of HEC errors reported on the port.
NUM of CHANGES	This output displays the number of changes to the port since initialization.
CARD DETECT	This output displays the number of new cards detected since the NI card became active.

Examples

The following example shows output from the **show dsl status cap** command:

```
DSLAM> show dsl status cap

Subtend Node ID: 0

                     DWNSTRM   UPSTRM  RCVR     TX    RCVR  UPSTRM     HEC   NUM of
  CARD
   NAME  ADMIN/OPER     (Kb)     (Kb)  GAIN  POWER     SNR  MARGIN  ERRORS  CHANGES
DETECT
   ----  ----------  -------  -------  ----  -----  ------  ------  ------  -------
------
 ATM4/1     UP/UP       7168     1088    6     20      45      11       0        5
     2
 ATM4/2     UP/UP       7168     1088    6     20      45      11       0       11
     2
 ATM4/3     UP/UP       7168     1088    6     20      45      11       0       13
     2
 ATM4/4     UP/UP       7168     1088    6     20      45      11       0        7
     2
```

Related Commands

Command	Description
show dsl status	Displays generic DSL interface information.

show dsl status dmt

To troubleshoot dmt ports, use the **show dsl status dmt** command.

show dsl status dmt

Syntax Description

The command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)DA	This command was modified to provide DMT specific feedback.

Usage Guidelines

Use this command to determine the administrative and operational status of each port. Nothing displays for slots that are empty and unprovisioned. This command also provides information on SNRs, HEC errors, line rates, receiver gain, and DMT cards detected.

Table 6-14 describes the fields shown in the display.

Table 6-14 show dsl status dmt Field Descriptions

Field	Description
NAME	This output displays the ATM slot(s) and ports.
ADMIN/OPER	This output displays whether the port is administratively up or down and whether the port is operationally (physically) up or down.
DWNSTRM INT (Kb)	If the port is configured for interleave path, this output displays the actual downstream data rate on the port.
UPSTRM INT (Kb)	If the port is configured for interleave path, this output displays the actual upstream data rate on the port.
DWNSTRM FST (Kb)	If the port is configured for fast path, this output displays the actual downstream data rate on the port.
UPSTRM FST (Kb)	If the port is configured for fast path, this output displays the actual upstream data rate on the port.
DWNSTRM MARGIN	This output displays the signal to noise margin of the signal that the port sends.
UPSTRM MARGIN	This output displays the signal to noise margin of the signal that the port receives.
FAR END ES	This output displays the number of errored seconds that the CPE reports.
NEAR END ES	This output displays the number of errored seconds that the port reports.

Table 6-14 show dsl status dmt Field Descriptions (continued)

Field	Description
NUM of CHANGES	This output displays the number of changes to the port since initialization.
CARD DETECT	This output displays the number of new cards detected since the NI card became active.

Examples

The following example shows output from the **show dsl status dmt** command:

```
DSLAM> show dsl status dmt

Subtend Node ID: 0

                 DWNSTRM UPSTRM DWNSTRM UPSTRM DWNSTRM UPSTRM  FAR    NEAR   NUM of   CARD
NAME  ADMIN/OPER INT(Kb) INT(Kb)FST(Kb) FST(Kb)MARGIN  MARGIN  END ES END ES CHANGE DETECT
----   ----------   -------    ------   -------    ------    ------   ------   ------
ATM1/1 UP/UP      0       0    8064    992    13.5     7.5     5        8        1       1
ATM1/2 UP/UP    8000   1024       0      0    11.0    13.5     1      136        1       1
```

Related Commands

Command	Description
show dsl status	Displays generic DSL interface information.

show dsl status idsl

To troubleshoot IDSL ports, use the **show dsl status idsl** command.

show dsl status idsl

Syntax Description

The command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.1(2)DA	This command was modified to provide IDSL specific feedback.

Usage Guidelines

Use this command to determine the administrative and operational status of each port. Nothing displays for slots that are empty and unprovisioned. This command also provides information on SNRs, HEC errors, line rates, receiver gain, and IDSL cards detected.

Table 6-15 describes the fields shown in the display.

Table 6-15 show dsl status idsl Field Descriptions

Field	Description
NAME	This output displays the ATM slot(s) and ports.
ADMIN/OPER	This output displays whether the port is administratively up or down and whether the port is operationally (physically) up or down.
RATE (Kb)	This output displays the actual data rate on the port.
FAR END SES	This output displays the number of severely errored seconds that the CPE reports.
FAR END ES	This output displays the number of errored seconds that the CPE reports.
NEAR END SES	This output displays the number of severely errored seconds that the port reports.
NEAR END ES	This output displays the number of errored seconds that the port reports.
NUM of CHANGES	Displays the number of changes to the port since initialization.
CARD DETECT	Displays the number of new cards detected since the NI card became active.

Examples

The following example shows output from the **show dsl status idsl** command:

```
DSLAM> show dsl status idsl

Subtend Node ID: 0

                    RATE      FAR     FAR     NEAR    NEAR  NUM of    CARD
   NAME  ADMIN/OPER (Kb)  END SES  END ES  END SES  END ES  CHANGE  DETECT
   ----  ---------- ----  -------  ------  -------  ------  ------  ------
IDSL2/1     UP/UP   144       2       6       1       8       2       1
IDSL2/2     UP/UP   144       2       6       1       8       2       1
IDSL2/3     UP/UP   144       2       6       1       8       2       1
IDSL2/4     UP/UP   144       2       6       1       8       2       1
```

Related Commands

Command	Description
show dsl status	Displays generic DSL interface information.

show dsl status sdsl

To troubleshoot SDSL ports, use the **show dsl status sdsl** command.

show dsl status sdsl

Syntax Description

The command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)DA	This command was modified to provide SDSL specific feedback.

Usage Guidelines

Use this command to determine the administrative and operational status of each port. Nothing displays for slots that are empty and unprovisioned. This command also provides information on SNRs, HEC errors, line rates, receiver gain, and SDSL cards detected.

Table 6-16 describes the fields shown in the display.

Table 6-16 show dsl status sdsl Field Descriptions

Field	Description
NAME	This output displays the ATM slot(s) and ports.
ADMIN/OPER	This output displays whether the port is administratively up or down and whether the port is operationally (physically) up or down.
RATE (Kb)	This output displays the actual data rate on the port.
RCVR GAIN	This output displays the DSLAM reporting of the amount of gain required to receive the signal. This number varies depending on signal attenuation and the transmit power of the CPE.
TX POWER	This output displays the amount of power that the DSLAM transmits out of the specific port.
RCVR SNR	This output displays the signal to noise margin of the signal that the port receives.
HEC ERROR	This output displays the number of HEC errors on the port.
NUM of CHANGES	This output displays the number of changes to the port since initialization.
CARD DETECT	This output displays the number of new cards detected since the NI card became active.

Examples

The following example shows output from the **show dsl status sdsl** command:

```
DSLAM> show dsl status sdsl

Subtend Node ID: 0
                                RATE   RCVR        TX      RCVR       HEC     NUM of       CARD
    NAME    ADMIN/OPER          (Kb)   GAIN     POWER       SNR     ERROR   CHANGES     DETECT
    ----    ----------       -------   ----    ------    ------    ------   -------     ------
  ATM3/1       UP/UP          1168      1        14        41         0         1          2
  ATM3/2       UP/UP          1168      1        14        41         0         2          2
```

Related Commands

Command	Description
show dsl status	Displays generic DSL interface information.

show dsl status shdsl

To troubleshoot shdsl ports, use the **show dsl status shdsl** command.

show dsl status shdsl

Syntax Description

The command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.1(7)DA2	This command was modified to provide G.SHDSL-specific feedback.

Usage Guidelines

Use this command to determine the administrative and operational status of each port. Nothing displays for slots that are empty and unprovisioned. This command also provides information on SNRs, HEC errors, line rates, receiver gain, and shdsl line cards detected.

Examples

The following example shows sample output from the **show dsl status shdsl** command:

```
DSLAM> show DSL status shdsl
Subtend Node ID: 0

                          RATE   RCVR    TX     RCVR     HEC   NUM of    CARD
   NAME   ADMIN/OPER      (Kb)   GAIN   POWER    SNR     ERROR  CHANGES  DETECT
    ----   ----------   -------  ----  ------   ------  ------ -------  ------
 ATM12/1    UP/  UP      1032    37      14       37       0       1        1
 ATM12/2    UP/  UP      1032    37      14       37       0       1        1
 ATM12/3    UP/  UP      1032    37      14       37       0       1        1
 ATM12/4    UP/  UP      1032    37      14       38       0       1        1
 ATM12/5    UP/  UP      1032    38      14       38       0       1        1
 ATM12/6    UP/  UP      1032    37      14       38       0       1        1
```

Command	Description
show dsl status	Displays generic DSL interface information.

show dsl test bert idsl

To view a bert test, use the **show dsl test bert idsl** command in EXEC configuration mode. The bert test command applies only to idsl ports and is activated by the **dsl test idsl bert** *slot#/port#* command in enabled mode.

show dsl test bert idsl *slot#/port#*

Syntax Description

The command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.1(2)DA	This command was modified to provide bert test feedback.

Usage Guidelines

Use this command to show the output for the BERT that is running on your system.

Table 6-17 describes the fields shown in the display.

Table 6-17 show dsl test bert Field Descriptions

Field	Description
Time remaining:	This output displays the time that remains on the current BERT.
Test duration:	This output displays the duration for a BERT. The default is 1 minute.
Total bits received:	This output displays the total number of bits received during testing.
Bit errors:	This output displays the number of bit errors as they occur during testing.
Sync count:	This output displays the actual number of sync losses thus far during the BERT.
Total sync time:	This output displays the amount of time that the line has been in sync during the test.
Current sync state:	This output displays whether the line is currently in sync.

Examples

The following example shows output from the **show dsl test bert idsl** 28/1 command:

```
DSLAM> show dsl test bert idsl 28/1
BERT is currently active on this interface
Time remaining : 00:00:27
Test duration : 1 minute(s)
Total bits received : 4753343
Bit errors : 49
Sync count : 7
```

```
Total sync time : 00:00:33
Current sync state : synced
```

After completion of the BERT:

```
DSLAM> show dsl test bert idsl 28/1
BERT is NOT currently active on this interface
Last BERT executed : 00:01:16
Test duration : 1 minute(s)
Total bits received : 8656695
Bit errors : 90
Sync count : 13
Total sync time : 00:01:00
```

Related Commands

Command	Description
dsl test idsl *slot#/port#* bert	Starts the BERT.

show environment

Use the **show environment** command in EXEC mode to display information about system temperature settings, as well as temperature details for installed cards or recently provisioned card slots.

show environment

Syntax Description

This command has no arguments or keywords.

Defaults

There is no default value for this command.

Command Modes

EXEC

Command History

Release	Modification
12.2(5)DA	This command was introduced.

Usage Guidelines

The **show environment** command displays information about system temperature settings on an installed card or the temperature details for a recently provisioned slot. The details display only if there is a temperature mismatch between the system and the slot components.

You can specify a temperature setting with the command:

set temperature-rating < commercial | osp >

Examples

In this example, the command displays temperature information for the system:

```
DSLAM#sh environment

Warning: Slot 2 Power Module is not present

Hardware temperature rating mismatches
System is provisioned as commercial:
Use SET command to change the provision of the system.
Hardware components NOT hardened(non-ITEMP):
ATUC-4FLEXIDMT                    C6160 fan tray
NI-2-155MM-155MM                  STUC-8-TCPAM
Hardware components hardened(ITEMP):
ATUC-8-DMT-1-H
```

Related Commands

Command	Description
set temperature-rating	Provisions the system temperature ratings. Systems are set as “commercial” by default.
show facility-alarm status	Displays current alarm information for your system.

show facility-alarm status

To display any current alarms on the system, use the **show facility-alarm status** command. Alarms matching selected severity or higher are displayed.

show facility-alarm status { critical | info | major | minor }

Syntax Description

critical	Shows critical facility alarms.
info	Shows all facility alarms.
major	Shows major and higher facility alarms.
minor	Shows minor and higher facility alarms.

Defaults

The default setting for this command is **info**.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

The **show facility-alarm status** command displays information about current alarms on your system.

Examples

In this example, the command displays current alarm information for the system:

```
DSLAM#sh facility-alarm status

System Totals  Critical: 2  Major: 0  Minor: 0
Source: Slot 1          Severity: INFO     Description: 4    Module was detected
Source: Slot 2          Severity: INFO     Description: 4    Module was detected
Source: Slot 3          Severity: INFO     Description: 4    Module was detected
Source: Slot 4          Severity: INFO     Description: 4    Module was detected
Source: Slot 5          Severity: INFO     Description: 4    Module was detected
Source: Slot 6          Severity: INFO     Description: 4    Module was detected
Source: ATM0/2          Severity: CRITICAL Description: 0    Loss of Signal
Source: ATM0/3          Severity: CRITICAL Description: 0    Loss of Signal
```

Related Commands

Command	Description
set temperature-rating	Provisions the system temperature ratings. Systems are set as “commercial” by default.
show interfaces	Displays interface configuration, status, and statistics.
show controllers atm	Displays debugging information for a port.

Command	Description
`show environment`	Displays information about system temperature settings, as well as temperature details for installed cards or recently provisioned card slots
`show dsl interface`	Displays DSL and ATM status for a port.

show hardware

Use the **show hardware** command to display information about the physical cards in the chassis and the chassis type and to determine whether the power supply and fan modules are present.

show hardware

show hardware slot *slot#*

show hardware chassis

Syntax Description

slot#	The slot number for which you want to show card information. The range is 1 to 38. (This is the maximum range; your chassis might have fewer than 38 slots.)

Defaults

There is no default value for this command.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

The **show hardware** command displays information about the cards in the chassis and the chassis type and indicates whether the power supply and fan modules are present.

In the event that the **show hardware** command detects a module mismatch, this command displays the mismatched card type, followed by the word "MISMATCH." See the "slot" section on page 7-4 for more information on card mismatches.

The **show hardware slot** command displays the name of the card in the specified slot, along with IDPROM contents (serial number, CLEI code, and so forth). For example: Slot 21: ATUC-1-4DMT, SERIAL #, H/W rev, S/W rev, CLEI code.

The **show hardware chassis** command displays the manufacturing information for the NI-2 motherboard, NI-2 daughter card, I/O controller, power module, backplane, chassis type and name, manufacturer name, H/W revision, Serial #, Asset ID, Alias, and CLEI code.

Note If a flexi line card displays as ATU-C Flex, that slot is unprovisioned and is nonoperational. You must use the **slot** command to provision the slot for either DMT or CAP line coding before the flexi line card becomes operational.

Examples

In this example, the command displays hardware information for the card in slot 4:

```
DSLAM> show hardware slot 4
```

Related Commands

Command	Description
show oir status	Displays the online insertion and removal (OIR) status of line card slots.
slot	Provisions a slot for a specific card type, or changes the line coding for a flexi line card. The **slot** command must be run in.

show hosts

To display the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of host names and addresses, use the **show hosts** EXEC command.

show hosts

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Examples

The following example displays a sample output from the **show hosts** command:

```
DSLAM> show hosts

Default domain is CISCO.COM
Name/address lookup uses domain service
Name servers are 255.255.255.255
Host              Flag        Age   Type       Address(es)
SLAG.CISCO.COM    (temp, OK)  1     IP         131.108.4.10
CHAR.CISCO.COM    (temp, OK)  8     IP         192.31.7.50
CHAOS.CISCO.COM   (temp, OK)  8     IP         131.108.1.115
DIRT.CISCO.COM    (temp, EX)  8     IP         131.108.1.111
DUSTBIN.CISCO.COM (temp, EX)  0     IP         131.108.1.27
DREGS.CISCO.COM   (temp, EX)  24    IP         131.108.1.30
```

Table 6-18 describes significant fields shown in the display.

Table 6-18 show hosts Field Descriptions

Field	Description
Flag	A temporary entry is made by a name server; the Cisco IOS software removes the entry after 72 hours of inactivity. A permanent entry is made by a configuration command and is not timed out. Entries marked OK are believed to be valid. Entries marked ?? are considered suspect and subject to revalidation. Entries marked EX are expired.
Age	Indicates the number of hours since the software last referred to the cache entry.
Type	Identifies the type of address, for example, IP, CLNS, or X.121. If you used the **ip hp-host** global configuration command, the **show hosts** command displays these host names as type HP-IP.
Address(es)	Displays the address of the host. One host can have up to eight addresses.

Related Commands

Command	Description
clear host	Deletes entries from the host-name-and-address cache.

show ima interface

To display the information about IMA groups and the links in those groups, use the **show ima interface** EXEC command.

show ima interface {**atm0/ima***ima-group-number* | **atm0**/*atm-interface-number* | **atm**}

Syntax Description

show ima interface	Displays information about all IMA groups and the links in those groups.
atm0/ima*ima-group-number*	Displays information about a single IMA group and the links in that group.
atm0/*atm-interface-number*	Displays IMA information for an individual link in an IMA group.
atm	Specifies an ATM interface.

Command Modes

EXEC

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

If you do not enter an ATM keyword, the **show ima interface** command displays all IMA interfaces that are present in the system.

Examples

This example shows sample output from the **show ima interface** command for ATM 0/IMA0.

```
DSLAM> show ima interface atm0/ima0
ATM0/IMA0 is up
        NeImaID = 0                     FeImaId = 0
    State:
        Ne = operational                Fe = operational
    Failure Status:
        Ne = noFailure
    Configuration:
        NumCfgLinks     = 2             MinNumLinks     = 2
        NeFrameLength   = m128          FeFrameLength   = m128
        NeTxClkMode     = ctc           FeTxClockMode   = ctc
        NeTimingRefLink = ATM0/2        FeTimingRefLink = ATM0/2
        NeOamLabel      = 1             FeOamLabel      = 1
        NeCTCLink       = ATM0/2
    Test:
        TestLink   = ATM0/2             TestPattern = 255
        TestStatus = disabled
    Performance:
        NumTxActLinks  = 2              NumRxActLinks   = 2
        DiffDelayMax   = 25             DiffDelayMaxObs = 0
        LeastDelayLink = ATM0/2
    IMA Group Counters:
        NeNumFailures    = 2            FeNumFailures   = 9
```

Table 6-19 describes some key fields in the **show ima interface** command displays.

Table 6-19 show ima interface Field Descriptions

Field	Description
MinNumTxLinks	Displays the minimum number of transmit links configured for the IMA group to function.
MinNumRxLinks	Displays the minimum number of receive links configured for the IMA group to function.
DiffDelayMax	Displays the maximum differential delay configured for the IMA group.
FrameLength	Displays the frame length configured for the IMA group.
NeTxClkMode	Displays the near-end transmit clock mode configured for the IMA group.
TestProcStatus	Displays the test procedure status configured for the IMA group.

Related Commands

Command	Description
show atm interface	Displays ATM-specific information about an ATM interface.
show interfaces	Displays the interface configuration, status, and statistics.

show interfaces

To display interface configuration, status, and statistics, use the **show interfaces** command.

show interfaces {*type* [*slot#/port#*[**:***cgn*] | **ima***group*]}

Syntax Description

type	Specifies one of the interface types listed in Table 6-20.
slot#/port#	Specifies the slot and port number of the ATM, CBR, or Ethernet interface.
:cgn	Specifies the channel-group number (identifier).
slot#/port#/**ima***group*	Specifies the slot, port, and IMA group number of the ATM interface.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

Table 6-20 shows the interface types for the **show interfaces** EXEC command.

Table 6-20 Interface Types for the show interfaces Command

Type	Description
atm	Specifies the ATM interface.
cbr	Specifies the CBR interface.
ethernet	Specifies the main Ethernet interface (0).
serial	Specifies a serial interface, such as a channelized Frame Relay interface.

Examples

The following is sample output from the **show interfaces atm** command for an IMA group interface:

```
DSLAM> show interfaces atm 0/ima0
ATM0/IMA0 is up, line protocol is up
  Hardware is t1_ima_group
  MTU 4470 bytes, sub MTU 4470, BW 3046 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
```

```
     0 output errors, 0 collisions, 4 interface resets
     0 output buffer failures, 0 output buffers swapped out
0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

The following is sample output for the **show interfaces atm** command for ATM 0/1:

```
DSLAM> show interfaces atm 0/1
ATM0/1 is up, line protocol is up
  Hardware is ds3suni
  MTU 4470 bytes, sub MTU 4470, BW 45000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     3236315 packets input, 171524695 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     3301762 packets output, 174047789 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

Table 6-21 lists the serial field descriptions for the **show interfaces** command.

Table 6-21 show interfaces serial Field Descriptions

Field	Description
MTU	Number of maximum transmission units.
BW	Number of bandwidth (kbps).
Dly	Number of the station delay parameter (used by IGRP).
relay	Number of the reliability coefficient.
load	Number of load (IGRP).
last input	Amount of time since last input in the following format: *hh:mm:ss.*
last output	Amount of time since last output in the following format: *hh:mm:ss.*
output hang	Time of last reset for output failure.
output queue	Size of output queue or default size of queue.
drops	Number of all output drops.
packets input	Number of all packets received since last reset.
bytes	Number of all bytes received since last reset.
no buffers	Number of all drops because of no buffers.
broadcasts, runts, giants	Not applicable if this is an ATM interface.
input errors	Number of damaged packets received.
crc	Number of packets received with correctable and uncorrectable input HCS errors.
frame	Number of packets with framing and alignment errors.
overrun, ignored, abort	Not applicable if this is an ATM interface.

Related Commands

Command	Description
show atm interface	Displays ATM-specific information about an ATM interface.

show ip bgp vpnv4

To display VPN address information from the Border Gateway Protocol (BGP) table, use the **show ip bgp vpnv4** EXEC command.

show ip bgp vpnv4 {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*}
[*ip-prefix/length* **[longer-prefixes] [***output-modifiers***]**]
[*network-address* **[***mask***] [longer-prefixes] [***output-modifiers***]**] [**cidr-only**] [**community**] [**community-list**] [**dampened-paths**] [**filter-list**] [**flap-statistics**] [**inconsistent-as**] [**neighbors**] [**paths** [*line*]] [**peer-group**] [**quote-regexp**] [**regexp**] [**summary**] [**tags**]

Syntax Description

all	Complete VPNv4 database.
rd *route-distinguisher*	Network Layer Reliability Information (NLRI) that has a matching route distinguisher.
vrf *vrf-name*	NLRI that is associated with the named VRF.
ip-prefix/length	(Optional) IP prefix address (in dotted-decimal format) and length of mask (0 to 32).
longer-prefixes	(Optional) The entry, if any, that exactly matches the specified prefix parameter, as well as all entries that match the prefix in a "longest-match" sense. That is, prefixes for which the specified prefix is an initial substring.
output-modifiers	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
network-address	(Optional) IP address of a network in the BGP routing table.
mask	(Optional) Mask of the network address, in dotted-decimal format.
cidr-only	(Optional) Only routes that have nonnatural net masks.
community	(Optional) Routes that matches this community.
community-list	(Optional) Routes that matches this community list.
dampened-paths	(Optional) Paths suppressed due to dampening (BGP route from peer is up and down).
filter-list	(Optional) Routes that conforms to the filter list.
flap-statistics	(Optional) Flap statistics of routes.
inconsistent-as	(Optional) Only routes that have inconsistent autonomous systems of origin.
neighbors	(Optional) Details about TCP and BGP neighbor connections.
paths	(Optional) Path information.
line	(Optional) A regular expression to match the BGP AS paths.
peer-group	(Optional) Information about peer groups.
quote-regexp	(Optional) Routes matching the AS path "regular expression."
regexp	(Optional) Routes matching the AS path regular expression.

summary	(Optional) BGP neighbor status.
tags	(Optional) Incoming and outgoing BGP labels for each NLRI.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

Use this command to display VPNv4 information from the BGP database. The command **show ip bgp vpnv4 all** displays all available VPNv4 information. The command **show ip bgp vpnv4 summary** displays BGP neighbor status.

Examples

The following example shows output for all available VPNv4 information in a BGP routing table:

```
DSLAM> show ip bgp vpnv4 all
BGP table version is 18, local router ID is 14.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP,? - incomplete

   Network          Next Hop Metric LocPrf Weight Path
Route Distinguisher: 100:1 (vrf1)
*> 11.0.0.0         50.0.0.1 0 0 101 i
*>i12.0.0.0         13.13.13.13 0    100 0 102 i
*> 50.0.0.0         50.0.0.1 0 0 101 i
*>i51.0.0.0         13.13.13.13 0    100 0 102 i
```

Table 6-22 describes the fields shown in this example.

Table 6-22 show ip bgp vpnv4 Field Descriptions

Field	Description
Network	Network address from the BGP table
Next Hop	Address of the BGP next hop
Metric	BGP metric
LocPrf	Local preference
Weight	BGP weight
Path	BGP path per route

The following example shows how to display a table of labels for NLRIs that have a route-distinguisher value of 100:1.

```
DSLAM> show ip bgp vpnv4 rd 100:1 tags
NetworkNext Hop      In tag/Out tag
Route Distinguisher: 100:1 (vrf1)
   2.0.0.0          10.20.0.60      34/notag
   10.0.0.0         10.20.0.60      35/notag
   12.0.0.0         10.20.0.60      26/notag
                    10.20.0.60      26/notag
   13.0.0.0         10.15.0.15      notag/26
```

Table 6-23 describes the fields shown in this example.

Table 6-23 show ip bgp vpnv4 rd Tags Field Descriptions

Field	Description
Network	Network address from the BGP table
Next Hop	BGP next hop address
In Tag	Label (if any) assigned by this router
Out Tag	Label assigned by the BGP next hop router

The following example shows VPNv4 routing entries for the VRF called vrf1.

```
DSLAM> show ip bgp vpnv4 vrf vrf1
BGP table version is 18, local router ID is 14.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP,? - incomplete

Network          Next Hop Metric LocPrf Weight Path
Route Distinguisher: 100:1 (vrf1)
*> 11.0.0.0         50.0.0.1 0 0 101 i
*>i12.0.0.0         13.13.13.13 0    100 0 102 i
*> 50.0.0.0         50.0.0.1 0 0 101 i
*>i51.0.0.0         13.13.13.13 0    100 0 102 i
```

Table 6-24 describes the fields shown in this example.

Table 6-24 show ip bgp vpnv4 Field Descriptions

Field	Description
Network	Network address from the BGP table
Next Hop	Address of the BGP next hop
Metric	BGP metric
LocPrf	Local preference
Weight	BGP weight
Path	BGP path per route

Related Commands

Command	Description
show ip vrf	Displays VRFs and associated interfaces.

show ip cef vrf

To display the Cisco Express Forwarding (CEF) forwarding table that is associated with a VRF, use the **show ip cef vrf** EXEC command.

show ip cef vrf *vrf-name* [*ip-prefix* [*mask* [**longer-prefixes**]] [**detail**] [*output-modifiers*]]
[*interface interface-number*] [**adjacency** [*interface interface-number*] [**detail**] [**discard**]
[**drop**] [**glean**] [**null**] [**punt**] [*output-modifiers*]] [**detail** [*output-modifiers*]]
[**non-recursive** [**detail**] [*output-modifiers*]] [**summary** [*output-modifiers*]]
[**traffic** [**prefix-length**] [*output-modifiers*]] [**unresolved** [**detail**] [*output-modifiers*]]

Syntax Description

vrf-name	Name assigned to the VRF.
ip-prefix	(Optional) IP prefix of entries to show, in dotted-decimal format (A.B.C.D).
mask	(Optional) Mask of the IP prefix, in dotted-decimal format.
longer-prefixes	(Optional) Table entries for all of the more specific routes.
detail	(Optional) Detailed information for each CEF table entry.
output-modifiers	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
interface	(Optional) Type of network interface to use: ATM, Ethernet, Loopback, POS (packet over SONET), or Null.
interface-number	Number identifying the network interface to use.
adjacency	(Optional) All prefixes resolving through adjacency.
discard	Discard adjacency.
drop	Drop adjacency.
glean	Glean adjacency.
null	Null adjacency.
punt	Punt adjacency.
non-recursive	(Optional) Only nonrecursive routes.
summary	(Optional) CEF table summary.
traffic	(Optional) Traffic statistics.
prefix-length	(Optional) Traffic statistics by prefix size.
unresolved	(Optional) Only unresolved routes.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

If you use this command with only the *vrf-name* argument, the **show ip cef vrf** command shows a shortened display of the CEF table.

If you use this command with the **detail** argument, the **show ip cef vrf** command shows detailed information for all CEF table entries.

Examples

This example shows the forwarding table associated with the VRF called vrf1.

```
DSLAM> show ip cef vrf vrf1
Prefix              Next Hop            Interface
0.0.0.0/32          receive
11.0.0.0/8          50.0.0.1            Ethernet1/3
12.0.0.0/8          52.0.0.2            POS6/0
50.0.0.0/8          attached            Ethernet1/3
50.0.0.0/32         receive
50.0.0.1/32         50.0.0.1            Ethernet1/3
50.0.0.2/32         receive
50.255.255.255/32   receive
51.0.0.0/8          52.0.0.2            POS6/0
224.0.0.0/24        receive
255.255.255.255/32  receive
```

Table 6-25 describes the fields shown in this example.

Table 6-25 show ip cef vrf Field Descriptions

Field	Description
Prefix	Network prefix
Next Hop	BGP next hop address
Interface	VRF interface

Related Commands

Command	Description
show ip route vrf	Displays the IP routing table that is associated with a VRF.
show ip vrf	Displays VRF interfaces.

show ip dhcp binding

To display address bindings on the Cisco IOS Dynamic Host Configuration Protocol (DHCP) server, use the **show ip dhcp binding** EXEC command.

show ip dhcp binding [*address*]

Syntax Description

address	(Optional) Specifies the IP address of the DHCP client for which bindings display.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

If you do not specify the address, all address bindings display. Otherwise, only the binding for the specified client displays.

Examples

The following examples show the DHCP binding address parameters, including an IP address, an associated MAC address, a lease expiration date, and the type of address assignments that have occurred. Table 6-26 describes the fields in each example.

```
DSLAM> show ip dhcp binding 172.16.1.11

IP address     Hardware address    Lease expiration      Type
172.16.1.11    00a0.9802.32de      Feb 01 1998 12:00 AM  Automatic

DSLAM> show ip dhcp binding 172.16.3.254

IP address     Hardware address    Lease expiration      Type
172.16.2.254   02c7.f800.0422      Infinite              Manual
```

Table 6-26 show ip dhcp Field Descriptions

Field	Description
IP address	The IP address of the host as recorded on the DHCP server.
Hardware address	The MAC address or client identifier of the host as recorded on the DHCP server.
Lease expiration	The lease expiration date of the IP address of the host.
Type	The manner in which the IP address was assigned to the host.

Related Commands

Command	Description
clear ip dhcp binding	Deletes an automatic address binding from the Cisco IOS DHCP server database.

show ip dhcp conflict

To display address conflicts found by a Cisco IOS Dynamic Host Configuration Protocol (DHCP) server when addresses are offered to the client, use the **show ip dhcp conflict** EXEC command.

show ip dhcp conflict [*address*]

Syntax Description

address	(Optional) Specifies the IP address of the conflict found.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The server detects conflicts using ping. The client detects conflicts using gratuitous Address Resolution Protocol (ARP). If either the server or the client detects an address conflict, the address is removed from the pool and the address is not assigned until an administrator resolves the conflict.

Examples

The following example displays the detection method and detection time for all IP addresses that the DHCP server has offered that have conflicts with other devices. Table 6-27 describes the fields in the example.

```
DSLAM> show ip dhcp conflict

IP address     Detection Method    Detection time
172.16.1.32    Ping                Feb 16 1998 12:28 PM
172.16.1.64    Gratuitous ARP      Feb 23 1998 08:12 AM
```

Table 6-27 show ip dhcp conflict Field Descriptions

Field	Description
IP address	The IP address of the host as recorded on the DHCP server.
Detection Method	The manner in which the IP addresses of the hosts were found on the DHCP server; this can be a ping or a gratuitous ARP.
Detection time	The time when the conflict was found.

Related Commands

Command	Description
clear ip dhcp conflict	Clears an address conflict from the Cisco IOS DHCP server database.
ip dhcp ping packets	Specifies the number of packets that a Cisco IOS DHCP server sends to a pool address as part of a ping operation.
ip dhcp ping timeout	Specifies how long a Cisco IOS DHCP server waits for a ping reply from an address pool.

show ip dhcp database

To display Cisco IOS Dynamic Host Configuration Protocol (DHCP) server database agent information, use the **show ip dhcp database** privileged EXEC command.

show ip dhcp database [*url*]

Syntax Description

url	(Optional) Specifies the remote file used to store automatic DHCP bindings. Following are the acceptable URL file formats: • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename

Defaults

If you do not specify a URL, all database agent records display. Otherwise, only information about the specified agent displays.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Examples

The following example shows all DHCP server database agent information. Table 6-28 describes each field in the example.

```
DSLAM> show ip dhcp database

URL         :   ftp://user:password@172.16.4.253/router-dhcp
Read        :   Dec 01 1997 12:01 AM
Written     :   Never
Status      :   Last read succeeded. Bindings have been loaded in RAM.
Delay       :   300 seconds
Timeout     :   300 seconds
Failures    :   0
Successes   :   1
```

Table 6-28 show ip dhcp database Field Descriptions

Field	Description
URL	Specifies the remote file used to store automatic DHCP bindings. The acceptable URL file formats include: • tftp://host/filename • ftp://user:password@host/filename • rcp://user@host/filename
Read	The last time bindings were read from the file server.

Table 6-28 show ip dhcp database Field Descriptions

Field	Description
Written	The last time bindings were written to the file server.
Status	Indication of whether the last read or write of host bindings was successful.
Delay	The amount of time to wait before updating the database.
Timeout	The amount of time before the file transfer is aborted.
Failures	The number of failed file transfers.
Successes	The number of successful file transfers.

Related Commands

Command	Description
ip dhcp database	Configures a DHCP server database agent and database agent parameters.

show ip dhcp server statistics

To display Cisco IOS Dynamic Host Configuration Protocol (DHCP) server statistics, use the **show ip dhcp server statistics** EXEC command.

show ip dhcp server statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Examples

The following example displays DHCP server statistics. Table 6-29 describes each field in the example.

```
DSLAM> show ip dhcp server statistics

Memory usage           40392
Address pools          3
Database agents        1
Automatic bindings     190
Manual bindings        1
Expired bindings       3
Malformed messages     0

Message                Received
BOOTREQUEST            12
DHCPDISCOVER           200
DHCPREQUEST            178
DHCPDECLINE            0
DHCPRELEASE            0
DHCPINFORM             0

Message                Sent
BOOTREPLY              12
DHCPOFFER              190
DHCPACK                172
DHCPNAK                6
```

Table 6-29 show ip dhcp server statistics Field Descriptions

Field	Description
Memory usage	The number of bytes of RAM allocated by the DHCP server.
Address pools	The number of configured address pools in the DHCP database.
Database agents	The number of database agents configured in the DHCP database.
Automatic bindings	The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.
Manual bindings	The number of IP addresses that have been manually mapped to the MAC addresses of hosts that are found in the DHCP database.
Expired bindings	The number of expired leases.
Malformed messages	The number of truncated or corrupted messages that were received by the DHCP server.
Message	The DHCP message type that was received by the DHCP server.
Received	The number of DHCP messages that were received by the DHCP server.
Sent	The number of DHCP messages that were sent by the DHCP server.

Related Commands

Command	Description
clear ip dhcp server statistics	Resets all Cisco IOS DHCP server counters.

show ip protocols vrf

To display the routing protocol information associated with a VRF, use the **show ip protocols vrf** EXEC command.

show ip protocols vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

Use this command to display routing information associated with a VRF.

Examples

The following example shows information about a VRF called vpn1.

```
DSLAM> show ip protocols vrf vpn2
Routing Protocol is “bgp 100"
  Sending updates every 60 seconds, next due in 0 sec
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Redistributing:connected, static
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
    13.13.13.13          200      02:20:54
    18.18.18.18          200      03:26:15
  Distance:external 20 internal 200 local 200
```

Table 6-30 describes the fields shown in this example.

Table 6-30 show ip protocols vrf Field Descriptions

Field	Description
Gateway	IP address of the router identifier for all routers in the network.
Distance	Metric used to access the destination route.
Last update	The last time the routing table was updated from the source.

Related Commands

Command	Description
show ip vrf	Displays VRF interfaces.

show ip route vrf

To display the IP routing table that is associated with a VRF (VPN routing or forwarding instance), use the **show ip route vrf** EXEC command.

show ip route vrf *vrf-name* [**connected**] [*protocol* [*as-number*] [*tag*] [*output-modifiers*]] [**list** *number* [*output-modifiers*]] [**profile**] [**static** [*output-modifiers*]] [**summary** [*output-modifiers*]] [**supernets-only** [*output-modifiers*]] [**traffic-engineering** [*output-modifiers*]]

Syntax Description

vrf-name	Name assigned to the VRF.
connected	All connected routes in a VRF.
protocol	To specify a routing protocol, use one of the following keywords: **bgp**, **egp**, **eigrp**, **igrp**, **isis**, **ospf**, or **rip**.
as-number	Autonomous system number.
tag	IOS routing area label.
output-modifiers	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
list *number*	IP access list to display.
profile	IP routing table profile.
static	Static routes.
summary	Summary of routes.
supernets-only	Supernet entries only.
traffic-engineering	Only traffic-engineered routes.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

This command displays specified information from the IP routing table of a VRF.

Examples

This example shows the IP routing table associated with the VRF called vrf1.

```
DSLAM> show ip route vrf vrf1
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, 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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route

Gateway of last resort is not set

B    51.0.0.0/8 [200/0] via 13.13.13.13, 00:24:19
C    50.0.0.0/8 is directly connected, Ethernet1/3
B    11.0.0.0/8 [20/0] via 50.0.0.1, 02:10:22
B    12.0.0.0/8 [200/0] via 13.13.13.13, 00:24:20
```

This example shows BGP entries in the IP routing table associated with the VRF called vrf1.

```
DSLAM> show ip route vrf vrf1 bgp
B  51.0.0.0/8 [200/0] via 13.13.13.13, 03:44:14
B  11.0.0.0/8 [20/0] via 51.0.0.1, 03:44:12
B  12.0.0.0/8 [200/0] via 13.13.13.13, 03:43:14
```

Related Commands

Command	Description
show ip cef vrf	Displays the CEF forwarding table associated with a VRF.
show ip vrf	Displays VRFs and associated interfaces.

show ip vrf

To display the set of defined VRFs (VPN routing or forwarding instances) and associated interfaces, use the **show ip vrf** EXEC command.

show ip vrf [{**brief | detail | interfaces}]** [*vrf-name*] [*output-modifiers*]

Syntax Description

brief	(Optional) Concise information on the VRFs and associated interfaces.
detail	(Optional) Detailed information on the VRFs and associated interfaces.
interfaces	(Optional) Detailed information about all interfaces bound to a particular VRF, or any VRF.
vrf-name	Name assigned to a VRF.
output-modifiers	(Optional) For a list of associated keywords and arguments, use context-sensitive help.

Defaults

When you do not specify any optional parameters, the command displays concise information about all configured VRFs.

Command Modes

EXEC

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

Use this command to display information about VRFs. Two levels of detail are available—use the **brief** keyword or no keyword to display concise information, or use the **detail** keyword to display all information. To display information about all interfaces bound to a particular VRF, or to any VRF, use the **interfaces** keyword.

Examples

This example shows brief information for the VRFs currently configured.

```
DSLAM> show ip vrf
  Name                Default RD          Interfaces
  vrf1                100:1               Ethernet1/3
  vrf2                100:2               Ethernet0/3
```

Table 6-31 describes the fields shown in this example.

Table 6-31 show vrf Field Descriptions

Field	Description
Name	VRF name
Default RD	Default route distinguisher
Interfaces	Network interfaces

This example shows detailed information for the VRF called vrf1.

```
DSLAM> show ip vrf detail vrf1
VRF vrf1; default RD 100:1
 Interfaces:
  Ethernet1/3
 Connected addresses are in global routing table
 Export VPN route-target communities
  RT:100:1
 Import VPN route-target communities
  RT:100:1
 No import route-map
```

Table 6-32 describes the fields shown in this example.

Table 6-32 show ip vrf detail Field Descriptions

Field	Description
Interfaces	Network interfaces
Export	VPN route-target export communities
Import	VPN route-target import communities

This example shows the interfaces bound to a particular VRF.

```
DSLAM> show ip vrf interfaces
Interface       IP-Address      VRF                     Protocol
Ethernet2       130.22.0.33     blue_vrf                up
Ethernet4       130.77.0.33     hub                     up
```

Table 6-33 describes the fields shown in this example.

Table 6-33 show ip vrf Interfaces Field Descriptions

Field	Description
Interface	Network interfaces for a VRF
IP-Address	IP address of a VRF interface
VRF	VRF name
Protocol	State of the protocol (up/down) for each VRF interface

Related Commands

Command	Description
ip vrf	Enters VRF configuration mode.
rd	Configures a default route distinguisher for a VRF.
route-target	Configures import and export extended community attributes for the VRF.
import	Configures an import route map for a VRF.
ip vrf forwarding	Associates a VRF with an interface or subinterface.

show oir status

To display the online insertion and removal (OIR) status of line card slots, use the **show oir status** exec command.

show oir status [*slot#*]

Syntax Description

slot#	(Optional) The slot number for which you want to show card information. The range is 1 to 38. (This is the maximum range; your chassis might have fewer than 38 slots.)

Defaults

If you omit *slot#*, the system displays the status of all the slots in the chassis.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

The **show oir status** command reports the status of line card slots in the DSLAM chassis. The reported status is one of the following:

- Loading—The line card in this slot is loading a new image, which typically takes about 2 minutes.
- Running—The line card in this slot is operating normally.
- Keepalive—The NI-2 is unable to communicate with the line card in this slot. The NI-2 keeps the line card in keepalive state for several seconds. If communication does not resume, the system assumes that the card was removed.

When the NI-2 cannot communicate with a line card, the NI-2 provides no entry for the slot where the card is located. The **show oir status** command displays a history of attempts to communicate with the line card.

After a 4xDMT line card has loaded a new image and **show oir status** indicates that it is running, the card might still be operationally down if the microcode is being updated. Use the **show dsl interface** command to examine the running card status.

Examples

The command in this example displays status information for all slots:

```
DSLAM> show oir status
```

Related Commands

Command	Description
show hardware	Displays information about the physical modules in the chassis.
show dsl interface atm	Displays DSL, DMT, CAP, and ATM status for a port.

show redundancy states

To display the state of the primary and secondary NI-2s, use the **show redundancy states** privileged EXEC command.

show redundancy states

Syntax Description

This command has no argument or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Usage Guidelines

This command displays the state of the primary and secondary NI-2s and identifies which NI-2 is active.

Table 6-34 describes the fields shown in the example.

Table 6-34 show redundancy states Field Descriptions

Field	Description
my state	The redundancy state of the active unit.
peer state	The redundancy state of the standby unit.
Mode	Simplex means that the standby unit is not installed or not yet detected. Duplex means that the standby unit is installed and functional.
Unit	The active unit. Primary is slot 10. Secondary is slot 11.
Split Mode	Enabled means that the secondary unit is logically disconnected from the active unit.
Manual Swact	Enabled means that you can manually switch from one unit to another.
Communications	The state of the communication link between the cards.
client count	The number of IOS features that have registered for redundancy services. This field is not user-configurable.
client_notification_TMR	The amount of time that IOS features registered for redundancy services have to respond to redundancy state changes. This field is not user-configurable.

Table 6-34 show redundancy states Field Descriptions (continued)

Field	Description
keep_alive TMR	The amount of time that the active card waits between sending consecutive keepalive messages. This field is not user-configurable.
keep_alive count	The number of keepalive messages that have been sent but have not yet received replies. This number should be 1 or 0. The count clears when a reply is received, so it increments only when consecutive keepalives do not receive replies. This field is not user-configurable.
keep_alive threshold	The number of keepalive messages that can be dropped before the active card decides that the standby card has failed and tries to reset it. This field is not user-configurable.

Examples

The following example shows sample output from the **show redundancy states** command:

```
DSLAM> enable
DSLAM# show redundancy states
my state =11 -ACTIVE
peer state = 8 -STANDBY READY
Mode = Duplex
Unit = Preferred Secondary
Split Mode = Disabled
Manual Swact = Enabled
Communications = Up
client count = 7
client_notification_TMR = 30000 milliseconds
keep_alive TMR = 2000 milliseconds
keep_alive count = 1
keep_alive threshold = 7
```

Related Commands

Command	Description
show aps	Displays the APS states of each SONET port on both NI-2 cards.
show controllers	Displays information on working and protection fibers.

show running-config

To display the running configuration for every currently defined profile, including the default profile, use the **show running-config** command.

show running-config

Syntax Description This command has no keywords or arguments.

Defaults There is no default value for this command.

Command Modes EXEC

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines This command tells you which ports are attached to each profile. Use **show dsl profile** to display configuration settings for selected profiles.

Examples In this example, the command shows the running configuration:

```
DSLAM> show running-config
```

Related Commands

Command	Description
dsl-copy-profile	Copies a DSL profile.
dsl-profile	Attaches a port to a profile.
show dsl profile	Displays a specific profile, all ports to which the profile is currently attached, and those port settings.
show startup-config	Displays the configuration file pointed to by the config_file environment variable.

show smb

To display the system management bus (SMB) error counters or the SMB utilization, use the **show smb** EXEC command. SMB errors are not relevant to subscriber traffic and have no effect on data path integrity.

show smb [errors | statistics]

Syntax Description

errors	Displays the SMB error counters.
statistics	Displays SMB statistics.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

Note SMB errors are not relevant to subscriber traffic and have no effect on data path integrity.

Examples

The following is sample output from the **show smb errors** command:

```
DSLAM#show smb errors
 SMB 0: 0 rxonly sent, 0 txonly sent, 17394199 txrx sent
         17394199 no response rcv'd from linecard, 0 short frames received
         0 length mismatches, 0 crc errors
         0 input fragments dropped
 SMB 1: 0 rxonly sent, 10008 txonly sent, 50538626 txrx sent
         66441 no response raved from linecard, 1783 short frames received
         19 length mismatches, 1 crc errors
 SMB 2: 0 rxonly sent, 10008 txonly sent, 61537964 txrx sent
         74816 no response rcv'd from linecard, 1111 short frames received
         11 length mismatches, 0 crc errors
```

The following is sample output from the **show smb statistics** command:

```
DSLAM#show smb statistics
SMB bus 0: utilization 63 percent.
SMB bus 1: utilization 12 percent.
SMB bus 2: utilization 19 percent.
```

Related Commands

None.

show snmp

To check the status of SNMP communications, use the **show snmp** EXEC command.

show snmp

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)DA	The command was introduced.

Usage Guidelines

This command provides counter information for SNMP operations.

Examples

The following example shows sample output from the **show snmp** command:

```
DSLAM> show snmp

Chassis: 01506199
37 SNMP packets input
    0 Bad SNMP version errors
    4 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    24 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    28 Get-next PDUs
    0 Set-request PDUs
78 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    24 Response PDUs
    13 Trap PDUs

SNMP logging: enabled
    Logging to 171.69.58.33.162, 0/10, 13 sent, 0 dropped.

SNMP Manager-role output packets
    4 Get-request PDUs
    4 Get-next PDUs
    6 Get-bulk PDUs
    4 Set-request PDUs
    23 Inform-request PDUs
    30 Timeouts
    0 Drops
SNMP Manager-role input packets
    0 Inform response PDUs
```

```
    2 Trap PDUs
    7 Response PDUs
    1 Responses with errors

SNMP informs: enabled
    Informs in flight 0/25 (current/max)
    Logging to 171.69.217.141.162
        4 sent, 0 in-flight, 1 retries, 0 failed, 0 dropped
    Logging to 171.69.58.33.162
        0 sent, 0 in-flight, 0 retries, 0 failed, 0 dropped
```

Table 6-35 describes the fields shown in the display.

Table 6-35 show snmp Field Descriptions

Field	Description
Chassis	Chassis ID string.
SNMP packets input	Total number of SNMP packets input.
Bad SNMP version errors	Number of packets with an invalid SNMP version.
Unknown community name	Number of SNMP packets with an unknown community name.
Illegal operation for community name supplied	Number of packets that request an operation not allowed for that community.
Encoding errors	Number of SNMP packets that were improperly encoded.
Number of requested variables	Number of variables requested by SNMP managers.
Number of altered variables	Number of variables altered by SNMP managers.
Get-request PDUs	Number of get requests received.
Get-next PDUs	Number of get-next requests received.
Set-request PDUs	Number of set requests received.
SNMP packets output	Total number of SNMP packets sent by the router.
Too big errors	Number of SNMP packets which were larger than the maximum packet size.
Maximum packet size	Maximum size of SNMP packets.
No such name errors	Number of SNMP requests that specified an MIB object which does not exist.
Bad values errors	Number of SNMP set requests that specified an invalid value for an MIB object.
General errors	Number of SNMP set requests that failed due to some other error. (It was not a noSuchName error, badValue error, or any of the other specific errors.)
Response PDUs	Number of responses sent in reply to requests.
Trap PDUs	Number of SNMP traps sent.
SNMP logging	Indicates whether logging is enabled or disabled.
sent	Number of traps sent.

Table 6-35 show snmp Field Descriptions (continued)

Field	Description
dropped	Number of traps dropped. Traps are dropped when the trap queue for a destination exceeds the maximum length of the queue, as set by the **snmp-server queue-length** command.
SNMP Manager-role output packets	Information related to packets sent by the router as an SNMP manager.
Get-request PDUs	Number of get requests sent.
Get-next PDUs	Number of get-next requests sent.
Get-bulk PDUs	Number of get-bulk requests sent.
Set-request PDUs	Number of set requests sent.
Inform-request PDUs	Number of inform requests sent.
Timeouts	Number of request timeouts.
Drops	Number of requests dropped. Reasons for drops include no memory, a bad destination address, or an unreasonable destination address.
SNMP Manager-role input packets	Information related to packets received by the router as an SNMP manager.
Inform response PDUs	Number of inform request responses received.
Trap PDUs	Number of SNMP traps received.
Response PDUs	Number of responses received.
Responses with errors	Number of responses containing errors.
SNMP informs	Indicates whether SNMP informs are enabled.
Informs in flight	Current and maximum possible number of informs waiting to be acknowledged.
Logging to	Destination of the following informs.
sent	Number of informs sent to this host.
in-flight	Number of informs currently waiting to be acknowledged.
retries	Number of inform retries sent.
failed	Number of informs that were never acknowledged.
dropped	Number of unacknowledged informs that were discarded to make room for new informs.

Related Commands

Command	Description
snmp-server chassis-id	Provides a message line identifying the SNMP server serial number.
session-timeout	Sets the amount of time before a nonactive session is destroyed.
snmp-server queue-length	Establishes the message queue length for each trap host.

show tag-switching forwarding vrf

To display label forwarding information for advertised VRF routes, use the **show tag-switching forwarding vrf** EXEC command. To disable the display of label forwarding information, use the **no** form of this command.

show tag-switching forwarding vrf *vrf-name* [*ip-prefix/length* [*mask*]] [**detail**] **[***output-modifiers*]

no show tag-switching forwarding vrf *vrf-name* [*ip-prefix/length* [*mask*]] [**detail**] **[***output-modifiers*]

Syntax Description

vrf-name	NLRIs associated with the named VRF.
ip-prefix/length	(Optional) IP prefix address (in dotted-decimal format) and length of mask (0 to 32).
mask	(Optional) Destination network mask, in dotted-decimal format.
detail	(Optional) Detailed information on the VRF routes.
output-modifiers	(Optional) For a list of associated keywords and arguments, use context-sensitive help.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.1(4)DA	This command was introduced.

Usage Guidelines

Use this command to display label forwarding entries associated with a particular VRF or IP prefix.

Examples

The following example shows label forwarding entries that correspond to the VRF called vpn1.

```
DSLAM> show tag-switching forwarding vrf vrf1 detail
```

Related Commands

Command	Description
show tag-switching forwarding	Displays label forwarding information.
show ip cef vrf	Displays VRFs and associated interfaces.

Shutdown Through V Commands for Cisco DSLAMs with NI-2

This chapter documents commands that you use to configure Cisco DSLAMs with NI-2. Commands in this chapter are listed alphabetically. For information on how to configure DSL features, refer to the *Configuration Guide for Cisco DSLAMs with NI-2*.

Note Commands that are identical to those documented in the *Cisco IOS Configuration Fundamentals Command Reference* and the *ATM and Layer 3 Switch Router Command Reference* have been removed from this chapter.

This chapter discusses the following commands:

shutdown

slot

snmp-server community

snmp-server contact

snmp-server enable traps

snmp-server host

snmp-server ifindex persist

snmp-server location

snmp-server queue-length

snmp trap link-status

sonet

source-ip

split-mode

subtend-id

tag-switching request-tags for

virtual-template

vpdn domain-delimiter

vpdn enable

vpdn-group

vpdn outgoing

vpdn source-ip

shutdown

To disable a port, use the **shutdown** command. To enable a port, use the **no** form of the command.

shutdown

no shutdown

Syntax Description

This command has no keywords or arguments.

Defaults

Enabled (no shutdown)

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

Use **shutdown** to disable a port. Use **no shutdown** to enable a disabled port.

Examples

In this example, the command enables slot 20, port 1:

```
DSLAM# configure terminal
DSLAM(config)# interface atm 20/1
DSLAM(config-if)# no shutdown
```

Related Commands

None.

slot

To provision a slot for a specific card type, or to change the line coding for a flexi line card, use the **slot** command.

slot *slot# cardtype*

Syntax Description

slot#	The number of the slot you want to provision. The range is 1 to 34. **Note** The number of slots varies by chassis. The Cisco 6015 has 6 slots, the Cisco 6160 has 32 slots, and the Cisco 6260 has 30 slots.
cardtype	The line card type for which you want to configure the slot. The valid card types are: • ATUC-1-4DMT—4xDMT card • ATUC-1-4DMT-I—4xDMT over ISDN card • ATUC-4FLEXICAP—4xflexi card configured as CAP • ATUC-4FLEXIDMT—4xflexi card configured as DMT • ATUC-1-DMT8—8xDMT card • ATUC-1-DMT8-I—8xDMT over ISDN card • ATUC-8-DMT-1-H—8xDMT OSP card • ITUC-1-8IDSL—8xIDSL card • STUC-4-2B1Q-DIR-1—4xSDSL card • STUC-8-TCPAM—8xSHDSL card **Note** Some line cards do not function in all NI-2 DSL systems. Consult the hardware documentation for your DSL system to determine which line cards it supports.

Defaults

There is no default value for this command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.1(1)DA	New card types were added.
12.1(6)DA	New card types were added.

Usage Guidelines

Use the **slot** command to provision a slot for a line card, and to provision a flexi line card for CAP or DMT line coding.

A card mismatch error condition can occur if the specified slot contains one type of card but is provisioned for another type.

If you attempt to provision an empty slot, the major alarm PROVISIONED SLOT IS EMPTY appears.

Note You must provision a 4xflexi line card for CAP or DMT line coding before it operates. After you provision the flexi card for CAP or DMT, the system downloads line card firmware to the flexi card. The download process takes about a minute. Do no remove the card, reboot the card, or reboot the system during the download.

The 4xflexi line card and the 8xDMT line card are spectrally incompatible with both the 8xIDSL line card and the 4xSDSL (STU-C) line card. If you install spectrally incompatible cards in the same side of the chassis, the lines served by those cards can suffer reduced performance. For best performance in a chassis with a mixture of line card types, always install flexi or DMT cards on one side of the chassis and install IDSL and SDSL cards on the opposite side.

Examples

The command in this example provisions slot 30 for a 4xflexi DMT line card.

```
DSLAM# configure terminal
DSLAM(config)# slot 30 ATUC-4FLEXIDMT
```

Related Commands

Command	Description
show hardware	Displays information about the physical modules in the chassis.

snmp-server community

To set up the community access string to permit access to the SNMP, use the **snmp-server community** global configuration command. The **no** form of this command removes the specified community string.

snmp-server community *string* [**view** *view-name*] [**ro** | **rw**] [*number*]

no snmp-server community *string*

Syntax Description

string	Community string that acts like a password and permits access to the SNMP.
view *view-name*	(Optional) Name of a previously defined view. The view defines the objects available to the community.
ro	(Optional) Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
rw	(Optional) Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.
number *<1-99>*	(Optional) Integer from 1 to 99 that specifies an access list of IP addresses that are allowed to use the community string to gain access to the SNMP agent.
number *<1300-1999>*	(Optional) Integer from 1300 to 1999 that specifies an expanded access list of IP addresses that are allowed to use the community string to gain access to the SNMP agent.

Defaults

By default, an SNMP community string permits read-only access to all objects.

Note If you do not use the **snmp-server community** command during the SNMP configuration session, this command is automatically added to the configuration after the **snmp-server host** command. In this case, the default password (*string*) for the **snmp-server community** is taken from the **snmp-server host** command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

The **no snmp-server** command disables all versions of SNMP (SNMPv1, SNMPv2C, SNMPv3).

The first **snmp-server** command that you enter enables all versions of SNMP.

Examples

The following example assigns the string **comaccess** to SNMP, allowing read-only access, and specifies that IP access list 4 can use the community string:

```
DSLAM(config)# snmp-server community comaccess ro 4
```

The following example assigns the string mgr to SNMP allowing read-write access to the objects in the restricted view:

```
DSLAM(config)# snmp-server community mgr view restricted rw
```

The following example removes the community comaccess:

```
DSLAM(config)# no snmp-server community comaccess
```

The following example disables all versions of SNMP:

```
DSLAM(config)# no snmp-server
```

Related Commands

Command	Description
access-list	Configures the access list mechanism to filter frames by protocol type or vendor code.

snmp-server contact

To set the system contact (sysContact) string, use the **snmp-server contact** global configuration command. Use the **no** form of the command to remove the system contact information.

snmp-server contact *text*

no snmp-server contact

Syntax Description

text	String that describes the system contact information.

Defaults

No system contact string is set.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Examples

The following example shows a system contact string:

```
DSLAM(config)# snmp-server contact Dial System Operator at beeper # 27345
```

Related Commands

Command	Description
snmp-server location	Sets the system location string.

snmp-server enable traps

To enable the DSLAM to send SNMP traps or informs (SNMP notifications), use the **snmp-server enable traps** global configuration command. Use the **no** form of this command to disable SNMP notifications.

snmp-server enable traps [*notification-type*] [*notification-option*]

no snmp-server enable traps [*notification-type*] [*notification-option*]

Syntax Description

notification-type (Optional) Type of notification to enable. If you do not specify a type, the software sends all notifications available on your device. The notification type can be one of the following keywords:

- **alarms**—Sends alarm notifications
- **atm-accounting**—Sends ATM Accounting notifications
- **atm-soft**—Sends ATM SoftVC notifications
- **config**—Sends configuration notifications.
- **entity**—Sends entity MIB modification notifications.
- **rtr**—Sends Service Assurance Agent/Response Time Reporter (RTR) notifications.
- **snmp [authentication]**—Sends RFC 1157 SNMP notifications. Use of the **authentication** keyword produces the same effect as not using the **authentication** keyword. Both the **snmp-server enable traps snmp** and **snmp-server enable traps snmp authentication** forms of this command globally enable (or, if you use the **no** form, disable) the following SNMP traps:
  - authentication failure
  - cold start
  - linkUp
  - linkDown
  - warmstart
- **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command.

Defaults

This command is disabled by default. Most notification types are disabled. However, you cannot control some notification types with this command.

If you enter this command with no *notification-type* keywords, the default is to enable all notification types that are controlled by this command.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

SNMP notifications are sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. To specify whether the notifications should be sent as traps or informs, use the **snmp-server host** [**traps** | **informs**] command.

If you do not enter an **snmp-server enable traps** command, no notifications controlled by this command are sent. In order to configure the DSLAM to send these SNMP notifications, enter at least one **snmp-server enable traps** command. If you enter the command with no keywords, all notification types are enabled. If you enter the command with a keyword, only the notification type related to that keyword is enabled. To enable multiple types of notifications, issue a separate **snmp-server enable traps** command for each notification type and notification option.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, configure at least one **snmp-server host** command.

For a host to receive a notification controlled by this command, both the **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. If the notification type is not controlled by this command, only the appropriate **snmp-server host** command must be enabled.

The notification types used in this command all have associated MIB objects that allow them to be globally enabled or disabled. Not all of the notification types available in the **snmp-server host** command have notificationEnable MIB objects, so some of these notification types cannot be controlled with the **snmp-server enable** command.

Examples

The following example enables the DSLAM to send all traps to the host specified by the name myhost.cisco.com, using the community string defined as public:

```
DSLAM(config)# snmp-server enable traps
DSLAM(config)# snmp-server host myhost.cisco.com public
```

The following example enables the DSLAM to send Frame Relay and environmental monitor traps to the host myhost.cisco.com using the community string public:

```
DSLAM(config)# snmp-server enable traps frame-relay
DSLAM(config)# snmp-server enable traps envmon temperature
DSLAM(config)# snmp-server host myhost.cisco.com public
```

The following example does not send traps to any host. The BGP traps are enabled for all hosts, but the only traps enabled to be sent to a host are ISDN traps (which are not enabled in this example).

```
DSLAM(config)# snmp-server enable traps bgp
DSLAM(config)# snmp-server host bob public isdn
```

The following example enables the DSLAM to send all inform requests to the host at the address myhost.cisco.com, using the community string defined as public:

```
DSLAM(config)# snmp-server enable traps
DSLAM(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example sends HSRP MIB traps to the host myhost.cisco.com using the community string public.

```
DSLAM(config)# snmp-server enable hsrp
DSLAM(config)# snmp-server host myhost.cisco.com traps version 2c public hsrp
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.

snmp-server host

To specify the recipient of an SNMP notification operation, use the **snmp-server host** global configuration command. To remove the specified host, use the **no** form of this command.

snmp-server host *host-addr* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]

no snmp-server host *host* [**traps** | **informs**]

Syntax Description

host-addr	Name or Internet address of the host (the targeted recipient).
traps	(Optional) Send SNMP traps to this host. This is the default.
informs	(Optional) Send SNMP informs to this host.
version	(Optional) Version of the Simple Network Management Protocol (SNMP) used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the **priv** keyword. If you use the **version** keyword, specify one of the following options: • **1**—SNMPv1. This option is not available with informs. • **2c**—SNMPv2C. • **3**—SNMPv3. The following three optional keywords can follow the version 3 keyword: – **auth** (optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication – **noauth** (default). The noAuthNoPriv security level. This is the default if the [auth | noauth | priv] keyword choice is not specified.
community-string	Password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host** command by itself, we recommend that you define this string using the **snmp-server community** command before you use the **snmp-server host** command.
udp-port *port*	UDP port of the host to use. The default is 162.

notification-type	(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords: • **alarms**—Sends alarm notifications • **atm-accounting**—Sends ATM Accounting notifications • **atm-soft**—Sends ATM SoftVC notifications • **config**—Sends configuration notifications. • **entity**—Sends entity MIB modification notifications. • **rtr**—Sends Service Assurance Agent (RTR) notifications. • **snmp**—Sends Simple Network Management Protocol (SNMP) notifications (as defined in RFC 1157). • **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command. • **tty**—Sends Cisco enterprise-specific notifications when a Transmission Control Protocol (TCP) connection closes. • **udp-port**—The notification host UDP port number

Defaults

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is version 1. The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

Note If you do not define the *community-string* with the **snmp-server community** command before you use this command, the default form of the **snmp-server community** command is automatically inserted into the configuration. The password (*community-string*) used for this automatic configuration of the **snmp-server community** is the same as that specified in the **snmp-server host** command. This is the default behavior for IOS Release 12.0(3) and later.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, but an inform can be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. In order to configure the DSLAM to send SNMP notifications, enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host.

To enable multiple hosts, issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When you issue multiple **snmp-server host** commands for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command replaces the first.

The **snmp-server host** command is used with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, enable at least one **snmp-server enable** command and the **snmp-server host** command for that host.

However, some notification types cannot be controlled with the **snmp-server enable** command. Some notification types are always enabled. Other notification types are enabled by a different command. For example, the linkUpDown notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

The availability of a notification-type option depends on the DSLAM type and Cisco IOS software features supported on the DSLAM. For example, the **envmon** notification-type is available only if the environmental monitor is part of the system.

Examples

If you want to configure a unique SNMP community string for traps, but you want to prevent SNMP polling access with this string, the configuration should include an access-list. In the following example, the community string is named “comaccess” and the access list is numbered 10:

```
DSLAM(config)# snmp-server community comaccess ro 10
DSLAM(config)# snmp-server host 172.20.2.160 comaccess
DSLAM(config)# access-list 10 deny any
```

The following example sends the SNMP traps to the host specified by the name myhost.cisco.com. The community string is defined as comaccess.

```
DSLAM(config)# snmp-server enable traps
DSLAM(config)# snmp-server host myhost.cisco.com comaccess snmp
```

The following example sends the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160:

```
DSLAM(config)# snmp-server enable traps
DSLAM(config)# snmp-server host 172.30.2.160 public snmp envmon
```

The following example enables the DSLAM to send all traps to the host myhost.cisco.com using the community string public:

```
DSLAM(config)# snmp-server enable traps
DSLAM(config)# snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host.

```
DSLAM(config)# snmp-server enable traps bgp
DSLAM(config)# snmp-server host bob public isdn
```

The following example enables the DSLAM to send all inform requests to the host myhost.cisco.com using the community string public:

```
DSLAM(config)# snmp-server enable traps
DSLAM(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example sends HSRP MIB traps to the host specified by the name myhost.cisco.com. The community string is defined as public.

```
DSLAM(config)# snmp-server enable hsrp
DSLAM(config)# snmp-server host myhost.cisco.com traps version 2c public hsrp
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server informs	Specifies inform request options.
snmp-server trap-source	Specifies the interface (and hence the corresponding IP address) from which an SNMP trap should originate.
snmp-server trap-timeout	Specifies the frequency for resending trap messages on the retransmission queue.

snmp-server ifindex persist

To globally enable ifIndex values to remain constant across reboots for use by SNMP, use the **snmp-server ifindex persist** command in global configuration mode. To globally disable ifIndex persistence, use the **no** form of this command in global configuration mode.

snmp-server ifindex persist

no snmp-server ifindex persist

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

Interface Index Persistence means that ifIndex values in the IF-MIB persist across reboots, allowing for consistent identification of specific interfaces that use SNMP.

The **snmp-server ifindex persist** global configuration command does not override an interface-specific configuration. Interface-specific configuration of ifIndex persistence is performed with the **[no] snmp ifindex persist** and **snmp ifindex clear** interface configuration commands.

The **[no] snmp-server ifindex persist** global configuration command enables and disables ifIndex persistence for all interfaces on the DSLAM using ifDescr and ifIndex entries in the ifIndex table of the IF-MIB.

Examples

In the following example, ifIndex persistence is enabled for all interfaces:

```
DSLAM(config)# snmp-server ifindex persist
```

In this example, if ifIndex persistence was previously disabled for a specific interface through the use of the **no snmp ifindex persist** interface configuration mode command, ifIndex persistence remains disabled for that interface. The global **ifIndex** command does not override the interface-specific commands.

Related Commands

Command	Description
snmp ifindex persist	Enables or disables ifIndex values in the IF-MIB that persist across reboots (ifIndex persistence) only on a specific interface.
snmp-server ifindex clear	Clears any interface-specific configuration of ifIndex persistence.

snmp-server location

To set the system location string, use the **snmp-server location** global configuration command. Use the **no** form of this command to remove the location string.

snmp-server location *text*

no snmp-server location

Syntax Description

text	String that describes the system location information.

Defaults

No system location string is set.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Examples

The following example shows a system location string:

```
DSLAM(config)# snmp-server location Building 3/Room 214
```

Related Commands

Command	Description
snmp-server contact	Sets the system contact (sysContact) string.

snmp-server queue-length

To establish the message queue length for each trap host, use the **snmp-server queue-length** global configuration command.

snmp-server queue-length *length*

Syntax Description

length	Integer that specifies the number of trap events that can be held before the queue must be emptied.

Defaults

10 events

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

This command defines the length of the message queue for each trap host. Once a trap message is successfully transmitted, the software continues to empty the queue, but never faster than at a rate of 4 trap messages per second.

Examples

The following example establishes a message queue that traps four events before it must be emptied:

```
DSLAM(config)# snmp-server queue-length 4
```

Related Commands

None.

snmp trap link-status

To enable SNMP link trap generation, use the **snmp trap link-status** interface configuration command. To disable SNMP link traps, use the **no** form of this command.

snmp trap link-status

no snmp trap link-status

Syntax Description

This command has no arguments or keywords.

Defaults

SNMP link traps are sent when an interface goes up or down.

Command Modes

Interface and profile configuration

Command History

Release	Modification
12.0(5)DA	This command was introduced.

Usage Guidelines

By default, SNMP link traps are sent when an interface goes up or down. For interfaces that are expected to go up and down during normal usage, such as ISDN interfaces, the output that these traps generate might not be useful. The **no** form of this command disables these traps.

Examples

The following example disables the sending of SNMP link traps related to the atm 0/1 interface:

```
DSLAM(config)# interface atm 0/1
DSLAM(config)# no snmp trap link-status
```

Related Commands

None.

sonet

To modify the framing mode for the interface, use the **sonet** interface configuration command.

sonet [stm-1 | sts-3c] [protection | working | <cr>]

Syntax Description

stm-1	Synchronous transfer mode-1.
sts-3c	Synchronous transport signal-3.
protection	The fiber that is local to the NI-2 card in slot 11.
working	The fiber that is local to the NI-2 card in slot 10.
<cr>	Both protection and working fibers.

Defaults

Default value is sts-3c.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Examples

The following example sets the framing mode to stm-1 on both the working and protection fibers:

```
DSLAM> enable
DSLAM# configure terminal
DSLAM(config)# interface atm 0/1
DSLAM(config-if)# sonet stm-1
```

Related Commands

Command	Description
show controllers	Displays information on working and protection fibers.

source-ip

To specify an alternate IP address for a VPDN tunnel that is different from the physical IP address used to open the tunnel, use the **source-ip** VPDN group command. To remove the alternate IP address, use the **no** form of this command.

source-ip *ip-address*

no source-ip

Syntax Description

ip-address	Alternate IP address (that is, different from the physical IP address used to open the VPDN tunnel) that the DSLAM uses to identify the tunnel.

Defaults

Disabled

Command Modes

VPDN group mode

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

You can configure each VPDN group on a DSLAM with a unique **source-ip** command.

Examples

The following example configures an L2TP access concentrator (LAC) to accept L2TP dial-out calls using the alternate IP address 172.23.33.7, which is different from the physical IP address used to open the L2TP tunnel.

```
DSLAM(config)# vpdn-group 3
DSLAM(config-vpdn)# accept-dialout
DSLAM(config-vpdn-acc-out)# protocol l2tp
DSLAM(config-vpdn-acc-out)# exit
DSLAM(config-vpdn)# source-ip 172.23.33.7
```

Related Commands

Command	Description
accept-dialin	Accepts requests to create either L2F or L2TP tunnels for dial-in.
accept-dialout	Accepts requests to tunnel L2TP dial-out calls.
request-dialin	Enables a DSLAM to request either L2F or L2TP tunnels for dial-in.
request-dialout	Enables a DSLAM to request L2TP tunnels for dial-out calls.

split-mode

To enter the redundancy submode to specify redundancy on NI-2s, use the **redundancy** global configuration command.

redundancy split-mode

Syntax Description

split-mode	Logically disconnect the secondary unit from the primary unit. This command is useful when you are performing software upgrades and other maintenance procedures. Use the **no** form of the command to reconnect the secondary unit and reset the standby unit.

Defaults

The default is no split-mode.

Command Modes

Redundancy submode

Command History

Release	Modification
12.1(7)DA	This command was introduced.

Usage Guidelines

If you use the redundancy command, you enter redundancy privileged EXEC submode (config-red). Within this submode, you can configure the redundancy-specific parameter for putting the system in split mode. To exit redundancy privileged EXEC submode, type exit.

If you disable split mode, the standby card is reloaded.

Examples

The following example puts the system into simplex mode:

```
DSLAM> enable
DSLAM# configure terminal
DSLAM(config)# redundancy
DSLAM(config-red)# split-mode
This command will place the system in SIMPLEX mode. [confirm] y
Secondary auto-sync disabled due to split-mode
```

Related Commands

Command	Description
show redundancy states	Display the state of the primary and secondary NI-2s, and identify which NI-2 is active.

subtend-id

To set the subtend node identifier, use the **subtend-id** command.

subtend-id *node#*

Syntax Description

node#	The identifier that you assign to this subtend node or to the specified subtend interface. The range is 0 to 12.

Defaults

The default subtend ID is 0 (zero).

Command Modes

Global configuration or interface configuration. See the Usage Guidelines below for details.

Command History

Release	Modification
12.0(5)DA	This command was introduced.
12.0(8)DA	The ability to assign a subtend ID to an interface was added.

Usage Guidelines

Assign to each subtended node a subtend identifier that is unique within its local subtend tree. If this condition is not met, some subscribers might not have fair access to the network.

The node at the top of the subtend tree—that is, the node that is connected to the trunk—must have the subtend ID 0. (Subtend ID 0 is the default.)

You can use the **subtend-id** command in global configuration mode or in interface configuration mode:

- Use it in global configuration mode to set the subtend ID of this chassis.
- Use it in interface configuration mode to assign a subtend ID to a subtended interface that is connected to a device that is not capable of assigning a subtend ID to itself—for example, a Cisco 6100 DSLAM. All the traffic that comes in through this interface will be tagged with the subtend ID that you assign to the interface, just as if the subtend ID had been assigned to the device connected to the interface. This feature allows otherwise incompatible devices to participate in a subtend tree.

Examples

The command in this example sets the subtend node identifier of this chassis to 12:

```
DSLAM# configure terminal
DSLAM(config)# subtend-id 12
```

The command in this example sets the subtend node identifier to 6 on port 0/2:

```
DSLAM# configure terminal
DSLAM(config)# interface atm 0/2
DSLAM(config-if)# subtend-id 6
```

Related Commands None.

tag-switching request-tags for

To restrict the creation of LVCs through the use of access lists on the LSC or label edge router, use the **tag-switching request-tags for** global configuration command. Use the **no** form of this command to disable this feature.

tag-switching request-tags for *access list*

no tag-switching request-tags for

Syntax Description

access list	A named or numbered standard IP access list.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

This command includes the following usage guidelines:

- You can specify either an access list number or a name.
- When you create an access list, the end of the access list contains an implicit deny statement for everything if the software did not find a match before reaching the end.
- If you omit the mask from an IP host address access list specification, 0.0.0.0 is assumed to be the mask.

Examples

This example shows how to prevent headend LVCs from being established from the LSC to all 198.x.x.x destinations. Add the following commands to the LSC configuration:

```
DSLAM(config)# tag-switching request-tags for 1
DSLAM(config)# access-list 1 deny 198.0.0.0 0.255.255.255
DSLAM(config)# access-list 1 permit any
```

Related Commands

Command	Description
access list	Creates access lists.
ip access-list	Permits or denies access to IP addresses.

virtual-template

To specify which virtual template to use to clone virtual-access interfaces, use the **virtual-template** accept-dialin command. To remove the virtual template from an accept-dialin VPDN subgroup, use the **no** form of this command.

virtual-template *template-number*

no virtual-template

Syntax Description

template number	Number of the virtual template to use to clone virtual-access interfaces.

Defaults

Disabled

Command Modes

Accept-dialin mode

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

Each accept-dialin group can clone virtual-access interfaces using only one virtual template. If you enter a second **virtual-template** command on an accept-dialin subgroup, it replaces the first virtual-template command.

You must first enable a tunneling protocol on the accept-dialin VPDN subgroup (using the **protocol** command) before you can enable the **virtual-template** command. If you remove or modify the **protocol** command, the **virtual-template** command is removed from the request-dialin subgroup.

Examples

The following example enables the LNS to accept an L2TP tunnel from a LAC named “mugsy.” A virtual-access interface will be cloned from virtual template 1:

```
DSLAM(config)# vpdn enable
DSLAM(config)# vpdn-group 1
(config-vpdn)# accept-dialin
(config-vpdn-acc-in)# protocol l2tp
(config-vpdn-acc-in)# virtual-template 1
```

Related Commands

Command	Description
accept-dialin	Accepts requests to create either L2F or L2TP tunnels for dial-in.

vpdn domain-delimiter

To specify the characters to be used to delimit the domain prefix or domain suffix, use the **vpdn domain-delimiter** global configuration command.

vpdn domain-delimiter *delimiter-characters* [**suffix** | **prefix**]

Syntax Description

delimiter-characters	One or more specific characters to be used as suffix or prefix diameters. Available characters are **%**, **–**, **@**, \ , **#**, and **/**. If a backslash (\) is the last delimiter in the command line, enter it as a double backslash (\\).
suffix | **prefix**	(Optional) Usage of the delimiter characters specified.

Defaults

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

You can enter one **vpdn domain-delimiter** command to list the suffix delimiters and another **vpdn domain-delimiter** command to list the prefix delimiters. However, no character can be both a suffix delimiter and a prefix delimiter.

This command allows the network access server to parse a list of home gateway DNS domain names and addresses sent by an AAA server. The AAA server can store domain names or IP addresses in the following AV pair:

```
cisco-avpair = "lcp:interface-config=ip address 1.1.1.1 255.255.255.255.0",
cisco-avpair = "lcp:interface-config=ip address bigrouter@excellentinc.com,
```

Examples

The following example lists three suffix delimiters and three prefix delimiters:

```
DSLAM(config)# vpdn domain-delimiter %-@ suffix
DSLAM(config)# vpdn domain-delimiter #/\\ prefix
```

Related Commands

Command	Description
vpdn enable	Enables VPDN on the DSLAM and informs the DSLAM to look for tunnel definitions in a local database and on a remote authorization server (LNS).
vpdn search-order	Specifies how the service provider network access server is to perform VPDN tunnel authorization searches.

vpdn enable

To enable VPDN on the DSLAM and inform the DSLAM to look for tunnel definitions in a local database, use the **vpdn enable** global configuration command. To disable VPDN, use the **no** form of this command.

vpdn enable

no vpdn enable

Syntax Description

This command has no keywords or arguments.

Defaults

Disabled

Command Modes

Global configuration.

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Examples

The following example enables VPDN on the router:

```
DSLAM(config)# vpdn enable
```

Related Commands

None.

vpdn-group

To define a local, unique group number identifier, use the **vpdn-group** global configuration command. To remove a group number, use the **no** form of this command.

vpdn-group *group-number*

no vpdn-group *group-number*

Syntax Description

group-number	Local group number. Valid group numbers range from 1 to 3000.

Defaults

VPDN group number assignments are not defined.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The **vpdn-group** command defines a local, unique identifier for each VPDN group.

Examples

The following example establishes local VPDN group number 1 for which other variables, such as force-local chap, can be assigned:

```
DSLAM(config)# vpdn enable
DSLAM(config)# vpdn group-number 1
```

Related Commands

None.

vpdn outgoing

To specify use of a domain name when selecting a tunnel for forwarding traffic to the remote host (the home gateway) on a virtual private dialup network, use the **vpdn outgoing** global configuration command.

vpdn outgoing {*domain-name*} *local-name* **ip** *ip-address*

Syntax Description

domain-name	Case-sensitive name of the domain to which traffic is forwarded.
local-name	Case-sensitive local name to use when authenticating the tunnel to the remote host.
ip *ip-address*	IP address of the remote host (home gateway).

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

The **request-dialin** command replaces this command.

The *domain-name* and *local-name* arguments are case sensitive.

This command is usually used on a network access server, not on a home gateway.

You can use the domain name to choose a tunnel destination. For example, if a user dials in as joe@company-a.com, where joe is the username and company-a.com is the domain name, you can select a tunnel destination based on the domain (company-a.com).

Note The **vpdn outgoing** command is still valid for defining tunnels; however, after you save the configuration, the user interface converts this command to the new syntax (the **request-dialin** command).

Examples

The following example selects a tunnel destination based on the domain name:

```
DSLAM(config)# vpdn enable
DSLAM(config)# vpdn outgoing chicago-main go-blue ip 172.17.33.125
```

Related Commands

Command	Description
vpdn enable	Enables VPDN on the DSLAM and informs the DSLAM to look for tunnel definitions in a local database and on a remote authorization server (LNS).
vpdn history failure table-size	Specifies the size of the user failure table.

vpdn source-ip

To set the source IP address of the network access server, use the **vpdn source-ip** global configuration command.

vpdn source-ip *address*

Syntax Description

address	IP address of the network access server.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(1b)DA	This command was introduced.

Usage Guidelines

One source IP address is configured on the network access server. The source IP address is configured per network access server, not per domain.

Examples

The following example enables VPDN on the network access server and sets an IP source address of 171.4.48.3.

```
DSLAM(config)# vpdn enable
DSLAM(config)# vpdn source-ip 171.4.48.3
```

Related Commands

None.

A

AAL5 ATM adaptation layer 5. This layer maps higher layer user data into ATM cells, making the data suitable for transport through the ATM network.

access identifier See *AID*.

address mask A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Sometimes called subnet mask.

ADSL asymmetric digital subscriber line. A digital subscriber line (DSL) technology in which the transmission of data from server to client is much faster than the transmission from the client to the server.

ADSL Transmission Unit—central office See *ATU-C*.

ADSL Transmission Unit—remote See *ATU-R*.

AID access identifier.

AIS alarm indication signal.

American National Standards Institute See *ANSI*.

American Wire Gauge See *AWG*.

ANSI American National Standards Institute. An organization that develops standards for many things, only some having to do with computers. ANSI is a member of the International Standards Organization (ISO). See *ISO*.

asymmetric digital subscriber line See *ADSL*.

asynchronous communications A method of transmitting data in which each transmitted character is sent separately. The character has integral start and stop bits so that the character can be sent at an arbitrary time, and separate from any other character.

Asynchronous Transfer Mode See *ATM*.

ATM Asynchronous Transfer Mode. A cell-based data transfer technique in which channel demand determines packet allocation. ATM offers fast packet technology, real time, demand led switching for efficient use of network resources.

ATM adaptation layer 5 See *AAL5*.

ATU-C ADSL Transmission Unit—central office.

ATU-R ADSL Transmission Unit—remote.

authentication A security feature that allows access to information to be granted on an individual basis.

autonegotiation Procedure for adjusting line speeds and other communication parameters automatically between two computers during data transfer.

AWG American Wire Gauge. The measurement of thickness of a wire.

B

bandwidth The range of frequencies a transmission line or channel can carry: the greater the bandwidth, the greater the information-carrying capacity of a channel. For a digital channel this is defined in bits. For an analog channel, it is dependent on the type and method of modulation used to encode the data.

bandwidth on demand The ability of a user to dynamically set upstream and downstream line speeds to a particular rate of speed.

BOOTP A TCP/IP network protocol that lets network nodes request configuration information from a BOOTP "server" node.

bps bits per second. A standard measurement of digital transmission speeds.

bits per second See *bps*.

bridge A device that connects two or more physical networks and forwards packets between them. Bridges can usually be made to filter packets, that is, to forward only certain traffic. Related devices are: repeaters which simply forward electrical signals from one cable to the other, and full-fledged routers which make routing decisions based on several criteria. See repeater and router.

broadband Characteristic of any network that multiplexes independent network carriers onto a single cable. This is usually done using frequency division multiplexing (FDM). Broadband technology allows several networks to coexist on one single cable; traffic from one network does not interfere with traffic from another since the "conversations" happen on different frequencies in the "ether" rather like the commercial radio system.

broadband remote access server Device that terminates remote users at the corporate network or Internet users at the ISP network that provides firewall, authentication, and routing services for remote users.

broadcast A packet delivery system where a copy of a given packet is given to all hosts attached to the network. Example: Ethernet.

C

CAP Carrierless Amplitude and Phase Modulation. A modulation technology for ADSL.

Carrierless Amplitude and Phase Modulation See *CAP*.

CBOS Cisco Broadband Operating System. Operating System that users access to configure and operate the Cisco products.

CCO Cisco Connection Online.

cell relay Generic term for a protocol based on small fixed packet sizes capable of supporting voice, video, and data at very high speeds.

central office See *CO*.

Channel Service Unit/Data Service Unit (CSU/DSU) A digital interface unit that connects end user equipment to the local digital telephone loop.

chassis The card cage (housing) where modules are placed.

Cisco Broadband Operating System See *CBOS*.

Cisco Connection Online See *CCO*.

CLEI Common Language Equipment Identifier.

client-server model A common way to describe network services and the user processes (programs) of those services. Examples include the name-server/name-resolver paradigm of the DNS and file-serve/file-client relationships such as NFS and diskless hosts.

CLI command line interface.

CLLI Common Language Location Identifier.

CO central office. Local telephone office through which all local loops in a given area connect and switch subscriber lines.

Common Language Equipment Identifier See *CLEI*.

Common Language Location Identifier See *CLLI*.

connectionless network The transport of a single datagram or packet of information from one network node to a destination node or multiple nodes without establishing a network connection.

connection-oriented network The transport of packets of information from one network node to a destination node following an established network connection.

CPE customer premises equipment. Terminating equipment, such as terminals, telephones, and modems, supplied by the telephone company. The equipment is installed at customer sites and connected to the telephone company network.

CTC common transmit clock.

customer premises equipment See *CPE*.

D

daemon A program that is not invoked explicitly but lies dormant waiting for some condition(s) to occur.

DDTS Cisco Distributed Defect Tracking System.

dial-up network Enables computer users to dial up a service provider's computer using a modem.

digital signal level 3 See *DS3*.

Discrete Multitone See *DMT*.

Distributed Defect Tracking System See *DDTS*.

distributed processing An approach that allows one application program to execute on multiple computers linked together by a network. The networked computers share the work between them.

DMT Discrete Multitone.

dotted decimal notation The syntactic representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 with periods (dots) separating them. Used to represent IP addresses in the Internet as in: 221.34.64.32.

downstream rate The line rate for return messages or data transfers from the network machine to the user's CPE.

DRAM dynamic random-access memory. A type of semiconductor memory in which the information is stored in capacitors on a metal oxide semiconductor integrated circuit.

DS1 digital signal level 1. A 1.544 Mbps digital signal that is carried on a T1 line.

DS3 digital signal level 3. Framing specification used for transmitting digital signals at 44.736 Mbps on a T3 facility.

DSLAM digital subscriber line access multiplexer. Concentrates and multiplexes digital subscriber line signals at the telephone service provider location to the broadband wide area network. Replaces ADSLAM.

DSL Forum An organization of competing companies that sponsors an Internet Web site (http://www.adsl.com) containing information about the applications, technology, systems, market, trials, and tariffs related to DSL technology.

dynamic random-access memory See *DRAM*.

E

E1 A digital carrier that is used to transmit a formatted signal at 2.048 Mbps.

EIA Electronic Industries Association. A standards organization made up of electronics industry organizations. EIA is responsible for The RS-232C and RS-422 standards.

Electronic Industries Association See *EIA*.

encapsulation The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the physical layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data.

entity A physical or logical system component which is represented in the 6100 SNMP Agent.

EPROM Erasable programmable read-only memory.

erasable programmable read-only memory See *EPROM*.

error detection A process used during file transfer to discover discrepancies between transmitted and received data. Some file transfer programs only detect errors; others detect errors and attempt to fix them (called error correction).

ESF Extended Superframe. A framing type that is used on T1 circuits that consists of 24 frames of 192 bits each, with the 193rd bit providing timing and other functions.

Ethernet One of the most common local area network (LAN) wiring schemes, Ethernet has a transmission rate of 10 Mbps; a newer standard called Fast Ethernet carries 100 Mbps.

ETSI A European standards body established in 1988 by a decision of the European Conference of Postal and Telecommunications Administrations (CEPT). It has taken over the work of the CEPT the area of developing the *Net-Normes Europeene de Telecommunication*, Net standards.

F

FCC Federal Communications Commission. A U.S. government agency that regulates interstate and foreign communications. The FCC sets rates for communication services, determines standards for equipment, and controls broadcast licensing.

Federal Communications Commission See *FCC*.

File Transfer Protocol See *FTP.*

finger daemon A software tool that allows a client to query a server for information on users.

firewall A method for protecting Internet-connected enterprise networks from break-ins by unauthorized persons outside the network.

frame A packet as it is transmitted over a serial line. The term derives from character oriented protocols where special start-of-frame and end-of-frame characters were added when transmitting packets.

FTP File Transfer Protocol. The Internet protocol (and program) used to transfer files between hosts.

G

G.804 ITU-T framing standard that defines the mapping of ATM cells into the physical medium.

gateway A system which does translation from some native format to another. Examples include X.400 to/from RFC 822 electronic mail gateways. See router.

H

handshake Part of the procedure to set up a data communications link. The handshake can be part of the protocol itself or an introductory process. The computers wishing to talk to each other set out the conditions they can operate under. Sometimes, the handshake is just a warning that a communication is imminent.

HDLC High-Level Data Link Control. A bit-oriented, synchronous, link layer, data-framing, flow control, and error detection and correction protocol. Available subsets include: 802.2 (logical link control for FDDI, Token Ring, and some Ethernet LANs, LAP (link access procedure balanced for X.25), LAPD (link access procedure for the ISDN D channel and frame relay), and LAPM (link access procedure for error-correcting modems specified as part of V.42).

High-Level Data Link Control See *HDLC*.

hop count A measure of distance between two points on the Internet. It is equivalent to the number of gateways that separate the source and destination.

HTML Hypertext Markup Language. The page-coding language for the World Wide Web.

HTML browser A browser used to traverse the Internet, such as Netscape or Microsoft Internet Explorer.

HTTP Hypertext Transfer Protocol. The protocol used to carry world wide web (WWW) traffic between a WWW browser computer and the WWW server being accessed.

Hypertext Markup Language See *HTML*.

Hypertext Transfer Protocol See *HTTP*.

ICMP Internet Control Message Protocol. The protocol used to handle errors and control messages at the IP layer.

ICP IMA control protocol.

IDCR IMA data cell rate.

IEEE Institute of Electrical and Electronics Engineers. A U.S. publishing and standards organization responsible for many LAN standards.

IMA inverse multiplexing over ATM. Standard protocol defined by the ATM Forum in 1997.

Industry-Standard Architecture See *ISA*.

Institute of Electrical and Electronics Engineers See *IEEE*.

International Organization for Standardization See *ISO*.

International Telecommunication Union Telecommunication Standardization Sector See *ITU-T*.

Internet A collection of networks interconnected by a set of routers, which allows them to function as a single, large virtual network. When written in upper case, Internet refers specifically to the DARPA (Defense Advanced Research Projects Agency) Internet and the TCP/IP protocols it uses.

Internet address An IP address assigned in blocks of numbers to user organizations accessing the Internet. The United States Department of Defense's Network Information Center establishes these addresses. Duplicate addresses can cause major problems on the network, but the NIC trusts organizations to use individual addresses responsibly. Each address is a 32-bit address in the form of x.x.x.x where *x* is an eight- bit number from 0 to 255. There are three classes: A, B, and C, depending on how many computers on the site are likely to be connected.

Internet Control Message Protocol See *ICMP*.

Internet Protocol See *IP*.

Internet service provider See *ISP*.

Internetwork Packet Exchange See *IPX*.

Internetwork Packet Exchange Control Protocol See *IPXCP.*

inverse multiplexing Allows individually dialed channels across the network to be combined into a single, higher-speed data streams. Using this service, a user can dial multiple calls and combine them together into a single high-speed data stream.

IP Internet Protocol. The network layer protocol for the Internet Protocol suite.

IP address The 32-bit address assigned to hosts that want to participate in a TCP/IP Internet.

IP datagram The fundamental unit of information passed across the Internet. It contains source and destination addresses along with data and a number of fields that define such things as the length of the datagram, the header checksum, and flags to say whether the datagram can be or has been fragmented.

IPX Internetwork Packet Exchange. The network layer (OSI Layer 3) datagram-based protocol usually used by Novell's NetWare network operating system. Supports any window size and packet sizes up to 64 KB.

IPXCP Internetwork Packet Exchange Control Protocol. A protocol defined in RFC 1552.

ISA Industry-Standard Architecture. The bus used in standard IBM-compatible PCs to provide power to add-in boards and to the motherboard (into which the boards plug). Typical maximum transfer speed of 1 to 2.5 Mbps (variables include other devices, memory, and buffering) but designed for up to 16 Mbps.

ISO International Organization for Standardization. A voluntary, nontreaty organization founded in 1946, responsible for creating international standards in many areas, including computers and communications.

ISP Internet service provider. A company that allows home and corporate users to connect to the Internet.

ITC independent transmit clock.

ITU-T International Telecommunication Union Telecommunication Standardization Sector. ITU-T is the telecommunication standardization sector of ITU and is responsible for making technical recommendations about telephone and data (including fax) communications systems for service providers and suppliers.

L

LAN local-area network. A limited distance (typically under a few kilometers or a couple of miles) high-speed network (typically 4 to 100 Mbps) that supports many computers (typically two to thousands).

LCD loss of cell delineation.

LCP link control protocol.

LED light emitting diode. The lights indicating status or activity on electronic equipment.

LIF loss of IMA frame.

light emitting diode See *LED*.

line concentration Functionality performed by a type of multiplexer that combines multiple channels onto a single transmission medium in such a way that all the individual channels can be simultaneously active. For example, ISPs use concentrators to combine their dial-up modem connections onto faster T1 lines that connect to the Internet.

line rate The speed by which data is transferred over a particular line type, express in bits per second (bps).

local-area network See *LAN*.

LODS loss of delay synchronization.

LOF loss of frame.

logical pool A logical grouping of ATU-C ports and LIM ports that comprise a particular DOH oversubscription ratio.

logical port A logical entry to a server machine. These ports are mostly invisible to the user, though you may occasionally see a URL with a port number included in it. These ports do not refer to physical locations; they are set up by server administrators for network trafficking.

loopback A diagnostic test that returns the transmitted signal back to the sending device after it has passed through a network or across a particular link. The returned signal can then be compared to the transmitted one. The discrepancies between the two help to trace the fault. When trying to locate a faulty piece of equipment, loopbacks will be repeated, eliminating satisfactory machines until the problem is found.

LOS loss of signal.

M

MAC Media Access Control. A sublayer of the Data Link Layer (Level Two) of the ISO OSI Model responsible for media control.

Management Information Base See *MIB*.

MD5 protocol Authentication and encryption protocol.

MDI Multidocument Interface.

Media Access Control See *MAC*.

MIB Management Information Base. A collection of objects that can be accessed via a network management protocol, such as SNMP and CMIP (Common Management Information Protocol).

MMF multimode fiber.

modem redundancy When backup modems are immediately available should a modem facilitating communication fail.

module A printed circuit board that occupies a slot in a chassis.

Multidocument Interface See *MDI*.

multimode fiber See *MMF*.

multicast A special form of broadcast where copies of the packet are delivered to only a subset of all possible destinations. See also *broadcast*.

multiplexer A device that can send several signals over a single line. They are then separated by a similar device at the other end of the link. This can be done in a variety of ways: time division multiplexing, frequency division multiplexing, and statistical multiplexing. Multiplexers are also becoming increasingly efficient in terms of data compression, error correction, transmission speed, and multidrop capabilities.

N

NAT Network Address Translation.

Network Address Translation See *NAT*.

network interface Boundary between a carrier network and a privately-owned installation.

network layer The OSI layer that is responsible for routing, switching, and subnetwork access across the entire OSI environment.

Network Virtual Terminal See *NVT*.

NI-2 A second generation network interface card.

node A general term used to refer to a computer or related device; often used to refer to a networked computer or device.

Node System Save file See *NSS*.

noise margin The amount of noise tolerated by the ATU-C and ATU-R while training.

NSS Node System Save file. The file that is saved during a Save Configuration or during a Software download. This file is required for Restore Configurations.

NVT Network Virtual Terminal.

O

OC-3 optical carrier level 3. Physical protocol, defined for SONET optical signal transmissions.

octet A networking term that identifies eight bits. In TCP/IP, it is used instead of *byte*, because some systems have bytes that are not eight bits.

OOF out of frame.

Open System Interconnection See *OSI*.

Optical Carrier Level 3 See *OC-3*.

OSI Open System Interconnection. An international standardization program to facilitate communications among computers from different manufacturers. See ISO.

OSR oversubscription ratio. The number of LIM ports divided by the number of ATU-C ports within a given logical pool.

oversubscription ratio See *OSR*.

P

packet The unit of data sent across a packet switching network.

PAP Password Authentication Protocol.

Password Authentication Protocol See *PAP*.

PCI Peripheral Component Interconnect. An industry local bus standard. Supports up to 16 physical slots but is electrically limited to typically three or four plug-in PCI cards in a PC. Has a typical sustained burst transfer rate of 80 Mb—enough to handle 24-bit color at 30 frames per second (full-color, full-motion video).

PEM power entry module.

Peripheral Component Interconnect See *PCI*.

permanent virtual circuit See *PVC*.

physical layer Handles transmission of raw bits over a communication channel. The physical layer deals with mechanical, electrical, and procedural interfaces.

physical pool A physical grouping of chassis slots within the Cisco 6100/6130 or Cisco 6110.

physical port A physical connection to a computer through which data flows. An “Ethernet port,” for example, is where Ethernet network cabling plugs into a computer.

plain old telephone service See *POTS*.

Point-to-Point Protocol See *PPP*.

port The abstraction used by Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host. A single termination point on one of the multiport modules (POTS, LIM, or ATU-C).

POTS plain old telephone service.

PPP Point-to-Point Protocol. The successor to SLIP, PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits. See SLIP.

protocol A formal description of messages to be exchanged and rules to be followed for two or more systems to exchange information.

PVC permanent virtual circuit. A fixed virtual circuit between two users: the public data network equivalent of a leased line. No call setup or clearing procedures are needed.

Q

QoS quality of service. A characteristic of data transmission that measures how accurately and how quickly a message or data is transferred from a source computer to a destination computer over a network.

quality of service See *QoS*.

R

RADIUS Remote Authentication Dial-In User Service. A client/server security protocol created by Livingston Enterprises. Security information is stored in a central location, known as the RADIUS server.

RADIUS Accounting Client Permits system administrators to track dial-in use.

RADIUS Security Client Controls access to specific services on the network.

RADSL rate adaptive digital subscriber line. A technique for keeping the quality of transmissions within specified parameters.

Rate Adaptive Digital Subscriber Line See *RADSL*.

remote address The IP address of a remote server.

Remote Authentication Dial-In User Service See *RADIUS*.

remote server A network computer that allows a user to log onto the network from a distant location.

Request for Comments See *RFC*.

RFC Request for Comments. The document series, begun in 1969, which describes the Internet suite of protocols and related experiments. Not all RFCs describe Internet standards, but all Internet standards are written up as RFCs.

route The path that network traffic takes from its source to its destination. The route a datagram may follow can include many gateways and many physical networks. In the Internet, each datagram is routed separately.

router A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this, it uses a routing protocol to gain information about the network and algorithms to choose the best route based on several criteria known as "routing metrics." See also *bridge*.

routing table Information stored within a router that contains network path and status information. It is used to select the most appropriate route to forward information along.

RS-232 An EIA standard that is the most common way of linking data devices together.

S

SAP Service Advertisement Protocol.

SDSL symmetrical digital subscriber line.

secret It is the encryption key used by RADIUS to send authentication information over a network.

serial line A serial line is used to refer to data transmission over a telephone line via a modem or when data goes from a computer to a printer or other device.

Service Advertisement Protocol See *SAP.*

shared secret RADIUS uses the shared secret to encrypt the passwords in the authentication packets, so outside parties do not have access to the passwords on your network.

signal-to-noise ratio See *SNR*.

SIMM Single In-line Memory Module. A small circuit board or substrate, typically about 10cm x 2cm, with RAM integrated circuits or die on one or both sides and a single row of pins along one long edge.

Simple Network Management Protocol See *SNMP.*

Single In-line Memory Module See *SIMM*.

single-mode fiber See *SMF.*

slot A numbered location within a chassis capable of housing a module.

SMF single-mode fiber.

SNMP Simple Network Management Protocol. The network management protocol of choice for TCP/IP-based internets.

SNR signal-to-noise ratio. Usable signal being transmitted divided by the noise or undesired signal.

socket (1) The Berkeley Unix mechanism for creating a virtual connection between processes. (2) IBM term for software interfaces that allow two Unix application programs to talk via TCP/IP protocols.

Spanning-Tree Protocol See *STP.*

spoofing A method of fooling network end stations into believing that keep-alive signals have come from and return to the host. Polls are received and returned locally at either end of the network and are transmitted only over the open network if there is a condition change.

STP Spanning-Tree Protocol. Part of an IEEE standard. A bridge protocol for detecting and preventing loops from occurring in a multibridged environment. When bridges connect three or more LAN segments, a loop can occur. Because a bridge forwards all packets which are not recognized as being local, some packets can circulate for long periods of time, eventually degrading system performance. This algorithm ensures only one path connects any pair of stations, selecting one bridge as the 'root' bridge, with the highest priority one as identifier, from which all paths should radiate.

STU-C SDSL Transmission Unit—central office.

subnet For routing purposes, IP networks can be divided into logical sub nets by using a subnet mask. Values below those of the mask are valid addresses on the subnet.

subnet mask See *address mask.*

subordinate entity An entity which has a superior entity.

subscriber A logical entity with attributes identifying the customer that is receiving service on a particular LIM port.

superior entity An entity which has subordinate entities.

SVC switched virtual circuit. A temporary virtual circuit between two users.

switch Equipment used to connect and distribute communications between a trunk line or backbone and individual nodes.

switched virtual circuit See *SVC.*

symmetrical digital subscriber line See *SDSL.*

synchronous connection During synchronous communications, data is not sent in individual bytes, but as frames of large data blocks.

SYSLOG SYSLOG allows you to log significant system information to a remote server.

T

T1 A digital carrier that is used to transmit a DS1 formatted digital signal at 1.544 Mbps.

T3 A digital carrier that is used to transmit a DS3 formatted digital signal at 45 Mbps.

TCP Transmission Control Protocol. The major transport protocol in the Internet suite of protocols providing reliable, connection-oriented full-duplex streams.

Telnet The virtual terminal protocol in the Internet suite of protocols. Allows users of one host to log into a remote host and act as normal terminal users of that host.

TFTP Trivial File Transfer Protocol. A simple file transfer protocol (a simplified version of FTP) that is often used to boot diskless workstations and other network devices such as routers over a network (typically a LAN). Has no password security.

training The procedure used by the ATU-C and ATU-R to establish an end-to-end ADSL connection.

training mode Characteristic of a router that allows it to use RADSL technology to adjust its line speed according to noise conditions on the transmission line.

Transmission Control Protocol See *TCP*.

transparent bridging So named because the intelligence necessary to make relaying decisions exists in the bridge itself and is thus transparent to the communicating workstations. It involves frame forwarding, learning workstation addresses and ensuring no topology loops exist (in conjunction with the Spanning-Tree algorithm).

Trivial File Transfer Protocol See *TFTP*.

twisted pair Two insulated copper wires twisted together with the twists or lays varied in length to reduce potential signal interference between the pairs.

U

UDP User Datagram Protocol. A connectionless transport protocol that runs on top of the TCP/IP IP. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagrams without acknowledgments or guaranteed delivery. Best suited for small, independent requests, such as requesting a MIB value from an SNMP agent, in which first setting up a connection would take more time than sending the data.

UL Underwriters Laboratories. A private organization that tests and certifies electrical components and devices against rigorous safety standards. A UL Listing Mark on a product means that representative samples of the product have been tested and evaluated to nationally recognized safety standards with regard to fire, electric shock, and other related safety hazards.

Underwriters Laboratories See *UL*.

UNI User-Network Interface.

UNI signaling User-Network Interface signaling for ATM communications.

upstream rate The line rate for message or data transfer from the source machine to a destination machine on the network. Also see downstream rate.

User Datagram Protocol See *UDP*.

V

VC virtual circuit. A logical circuit created to ensure reliable communication between two network devices. A virtual circuit is defined by a VPI/VCI pair, and can be either permanent (PVC) or switched (SVC). In ATM, a virtual circuit is called a virtual channel. Sometimes abbreviated VC. See also *PVC*, *SVC*, *VCI*, and *VPI*.

VCC virtual channel connection. Logical circuit, made up of links, that carries data between two end points in an ATM network. Sometimes called a virtual channel connection. See also *VCI* and *VPI*.

VCI virtual channel identifier. 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through to the ATM switch. Sometimes called virtual channel connection. See also *VPI*.

virtual channel See *VC*.

virtual circuit See *VC*.

virtual channel connection See *VCC*.

virtual channel identifier See *VCI*.

virtual connection In ATM, a connection between end users that has a defined route and endpoints. See also *PVC* and *SVC*.

virtual path A logical grouping of virtual circuits that connect two sites. See also *virtual circuit*.

virtual path identifier See *VPI*.

virtual path identifier/virtual circuit identifier See *VPI* and *VCI*.

VP virtual path. One of two types of ATM circuits identified by a VPI. A virtual path is a bundle of virtual circuits, all of which are switched across a network based on a common VPI. See also *VPI*.

VPI virtual path identifier. An 8-bit field in the header of an ATM cell. The VPI, together with the VCI, is used to identify the next destination of a cell as it passes through the network. See also *VCI*.

W

WAN wide-area network. A data communications network that spans any distance and is usually provided by a public carrier (such as a telephone company or service provider).

wide-area network See *WAN*.

Symbols

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W