CISCO SYSTEMS

Cisco 6400 Command Reference

June 2003

CONTENTS

CHAPTER 1 **Commands for the Cisco 6400 NRP** **1-1**

Preface

This preface describes the objectives, organization, and audience of this command reference, as well as conventions and related documentation.

Document Objectives

This document lists the Cisco IOS commands that were specifically created or modified for the Cisco6400 carrier-class broadband aggregator. Additional commands used to configure the node route processor (NRP) are described in the Cisco IOS Command Reference publications; additional commands used to configure the node switch processor (NSP) are described in the *ATM and Layer 3 Switch Router Command Reference.* All documents are available on Cisco.com or on the Cisco Documentation CD-ROM.

Related Documentation

To complement the software information provided in this command reference, refer to the following documents:

Cisco6400 *Software Setup Guide*—perform basic configurations and set up connectivity among the Cisco6400 components.

Cisco6400 *Feature Guide*—Lists the many features supported by the Cisco6400, provides references to cross-platform feature documentation, and describes deployment of features that are unique to the Cisco6400.

ATM Switch Router Software Configuration Guide—Describes additional ATM features and functionality that are supported by the Cisco6400 node switch processor (NSP).

ATM and Layer 3 Switch Router Command Reference—Describes additional commands supported by the Cisco6400 NSP.

Cisco IOS Configuration Guides and Command References—Describes extensive Cisco IOS features and commands that apply to most Cisco products, including the Cisco6400.

Audience

This command reference is designed for system administrators who are responsible for setting up the CiscoIOS software on the Cisco6400 and are familiar with the installation of high-end networking equipment.

This command reference is intended primarily for the following audiences:

- Customers with technical networking background and experience.
- Customers who support dial-in users.
- System administrators who are familiar with the fundamentals of router-based internetworking, but who may not be familiar with CiscoIOS software.
- System administrators who are responsible for installing and configuring internetworking equipment, and who are familiar with Cisco IOS software.

Documentation Conventions

For more information on the layout of this Command Reference, see the "Using Cisco IOS Software" chapter of the *Cisco IOS Configuration Fundamentals Command Reference*:

This section describes the following conventions used by this command reference:

- Command Syntax
- Examples
- Keyboard
- Notes, Timesavers, Tips, and Cautions

Command Syntax

Convention	Description
boldface	Indicates commands and keywords that are entered literally as shown.
italics	Indicates arguments for which you supply values; in contexts that do not allow italics, arguments are enclosed in angle brackets (< >).
[**x**]	Keywords or arguments that appear within square brackets are optional.
{**x** | **y** | **z**}	A choice of required keywords (represented by **x**, **y**, and **z**) appears in braces separated by vertical bars. You must select one.
[**x** {**y** | **z**}]	Braces and vertical bars within square brackets indicate a required choice within an optional element. You do not need to enter the optional element. If you do, you have some required choices.

Examples

Convention	Description
screen	Shows an example of information displayed on the screen.
boldface screen	Shows an example of information that you must enter.
< >	Nonprinting characters, such as passwords, appear in angled brackets.
!	Exclamation points at the beginning of a line indicate a comment line. Exclamation points are also displayed by the Cisco IOS software for certain processes.
[ ]	Default responses to system prompts appear in square brackets.
prompt> prompt#	Examples that contain system prompts denote interactive sessions, indicating the commands that you should enter at the prompt. The system prompt indicates the current level of the EXEC command interpreter. For example, the prompt router> indicates that you should be at the user level, and the prompt router# indicates that you should be at the privileged level. Access to the privileged level usually requires a password.

Keyboard

Convention	Description
Z	Keys are indicated in capital letters but are not case sensitive.
^ or Ctrl	Represents the Control key. For example, when you read *^D or Ctrl-D*, you should hold down the Control key while you press the D key.

Notes, Timesavers, Tips, and Cautions

The following conventions are used to attract the reader's attention:

Note Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Tip Means *the following information might help you solve a problem*.

Caution Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped 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 408526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408527-0730.

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

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: 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 by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity

- Resolve technical issues with online support

- Download and test software packages

- Order Cisco learning materials and merchandise

- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC WebSite and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.

- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.

- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.

- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

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

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

1

Commands for the Cisco 6400 NRP

This chapter describes the commands specific to the Cisco 6400 node route processor (NRP) except **show** commands, which are described in Chapter 2, "Show Commands for the Cisco 6400 NRP"

Additional commands used to configure the NRP are described in the Cisco IOS command reference publications, available on Cisco.com or on the Documentation CD-ROM.

Tasks are presented only in the context of using a particular command; this chapter does not describe how the tasks interrelate, nor does it provide comprehensive configuration examples.

accept dialin

To specify the virtual template to use for cloning new virtual-access interfaces when an incoming tunnel connection is requested from a specific peer, use the **accept dialin** VPDN group command. To disable authentication and virtual template cloning, use the **no** form of this command.

accept dialin [**l2f** | **l2tp** | **any** | **pppoe**] **virtual-template** *number* [**remote** *remote-peer-name*]

no accept dialin [**l2f** | **l2tp** | **any** | **pppoe**] **virtual-template** *number* [**remote** *remote-peer-name*]

Syntax DescriptionS		
l2f	**l2tp**	**any**	**pppoe**	(Optional) Indicates which protocol to use for a dial-in tunnel.
		l2f—Layer 2 Forwarding protocol.
		l2tp—Layer 2 Tunnel Protocol.
		any—VPDN will use autodetect to select either L2F or L2TP. Does not apply to PPPoE.
		pppoe—Point-to-Point Protocol over Ethernet.
virtual-template *number*		The virtual template interface from which the new virtual-access interface is cloned.
remote *remote-peer-name*		(Optional) Case-sensitive name that the remote peer will use for identification and tunnel authentication. Does not apply to PPPoE.

Syntax Description   Disabled

Command Modes   VPDN group mode

Command History

Release	Modification
10.0	This command was introduced.
11.3(3)T	The **log** keyword was added.
12.0(1)T	This command was modified.
12.0(3)DC	The **pppoe** keyword was added on the Cisco 6400 NRP.

Usage Guidelines   This command replaces the **vpdn incoming** command used in Cisco IOS Release 11.3. The user interface will automatically be upgraded when you reload the router with a 12.0 T image.

When used with L2F or L2TP, the router replies to a dial-in Layer 2 tunnel open request from the specified peer. When the access server accepts the request, the router uses the specified virtual template to clone new virtual-access interfaces.

Note   The Cisco 6400 does not support L2F.

When used with PPPoE, the **accept dialin** command enables the router to accept incoming PPPoE discovery packets from clients and establish PPPoE sessions with them. After the PPPoE discovery stage is completed, PPPoE uses the specified virtual template to clone new virtual-access interfaces. If a pre-cloned virtual-access interface is available in PPPoE private list, PPPoE uses that virtual-access interface to establish a PPP session with the client.

Note Configure the **vpdn-group** command with the **accept dialin** or **request dialin** command.

Examples This example shows how to allow an access server to accept a PPPoE dial-in tunnel. A virtual-access interface will be cloned from virtual-template 1:

accept dialin pppoe virtual-template 1

If you use the **accept dialin** command with the pppoe and virtual-template keywords and omit the remote-peer-name argument, you automatically enable a default PPPoE VPDN group, which allows all tunnels to share the same tunnel attributes:

vpdn-group 1
! Default PPPoE VPDN group
 accept dialin pppoe virtual-template 1

Related Commands

Command	Description
vpdn incoming	Specifies the local name to use for authenticating, and the virtual template to use for building interfaces for incoming connections.

atm route-bridge

To configure an interface to use ATM routed bridging, use the **atm route-bridge** interface configuration command.

atm route-bridge *protocol*

Syntax Description

protocol	Protocol to be route-bridged.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples

This example shows how to configure ATM routed bridging on an interface:

```
Router(config)# interface atm 4/0.100 point-to-point
Router(config-if)# ip address 172.69.5.9 255.255.255.0
Router(config-if)# pvc 0/32
Router(config-if)# atm route-bridged ip
```

atm vc tx

To set the PVC segmentation buffer size, use the **atm vc tx** interface configuration command. To revert to the default value of 32, use the **no** form of this command.

atm vc tx *queue-depth*

no atm vc tx *queue-depth*

Syntax Description		
queue-depth	Maximum number of packets in the buffer queue. Possible values: 32, 64, 128, 256.	

Defaults   32

Command Modes   ATM VC

Command History

Release	Modification
12.1(1)DC1	This command was introduced on the Cisco 6400 NRP.
12.2(4)B	The service internal requirement was removed.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   For each PVC, a segmentation buffer slot is reserved for high-priority packets.

⚠

Caution   Entering the **atm vc tx** command can cause service disruption. Only enter this command during maintenance windows.

Examples   This example shows how to set the maximum number of packets in the segmentation buffer of each PVC to 64:

```
!
interface atm 0/0/0
  atm vc tx 64
!
```

Related Commands

Command	Description
interface atm	Configures an ATM interface type and enters interface configuration mode.

attribute

To configure an attribute in a local service profile, use the **attribute** profile configuration command. Use the **no** form of this command to delete an attribute from a service profile.

attribute *radius-attribute-id* [*vendor-id*] [*cisco-vsa-type*] *attribute-value*

no attribute *radius-attribute-id* [*vendor-id*] [*cisco-vsa-type*] *attribute-value*

Syntax Description

radius-attribute-id	RADIUS attribute ID to be configured.
vendor-id	(Optional) Vendor ID. Required if the RADIUS attribute ID is 26, indicating a vendor-specific attribute. Cisco's vendor ID is 9.
cisco-vsa-type	(Optional) Cisco vendor-specific attribute (VSA) type. Required if the vendor ID is 9, indicating a Cisco VSA.
attribute-value	Attribute value.

Defaults   No default behavior or values.

Command Modes   Profile configuration

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   Use this command to configure attributes in local service profiles.

For the SSG Open Garden feature, use this command to configure the Service Route, DNS Server Address, and Domain Name attributes in a local service profile before adding the service to the open garden.

Examples   In the following example, the Cisco-AVpair Upstream Access Control List (inacl) attribute is configured in the local service profile called cisco.com:

```
Router(config)# local-profile cisco.com
Router(config-prof)# attribute 26 9 1 "ip:inacl#101=deny tcp 10.2.1.0 0.0.0.255 any eq 21"
```

In the following example, the Session-Timeout attribute is deleted from the local service profile called cisco.com:

```
Router(config)# local-profile cisco.com
Router(config-prof)# no attribute 27 600
```

In the following example, an open garden service called "opencisco.com" is defined.

```
Router(config)# local-profile opencisco.com
Router(config-prof)# attribute 26 9 251 "Oopengarden1.com"
Router(config-prof)# attribute 26 9 251 "D10.13.1.5"
Router(config-prof)# attribute 26 9 251 "R10.1.1.0;255.255.255.0"
Router(config-prof)# exit
Router(config)# ssg open-garden opencisco.com
```

Related Commands

Command	Description
local-profile	Configures a local service profile.
show ssg open-garden	Displays a list of all configured open garden services.
ssg open-garden	Designates a service, defined in a local service profile, to be an open garden service.

debug pmbox

To display debug messages for traffic flowing on the NRP-2 PAM mailbox serial interface, use the **debug pmbox** EXEC command. The **no** form of this command disables debugging output.

debug pmbox {events | {rx-path | tx-path} {all | config-download | config-update | diag | driver | ehsa | force-fail | image-download | info-request | nrp | ping | status-update | syslog | test1 | test2 | xc-request | xc-response}}

no debug pmbox {events | {rx-path | tx-path} {all | config-download | config-update | diag | driver | ehsa | force-fail | image-download | info-request | nrp | ping | status-update | syslog | test1 | test2 | xc-request | xc-response}}

Syntax Description

events	Displays PAM mailbox messaging events. Traces routine execution as message are moved from one CPU to another.
rx-path	Selects messages received by the PAM mailbox serial interface from the NSP.
tx-path	Selects messages transmitted by the PAM mailbox serial interface to the NSP.
all	Displays all messages.
config-download	Displays configuration download messages.
config-update	Displays configuration update messages.
diag	Displays diagnostic messages.
driver	Displays driver messages.
ehsa	Displays enhanced high system availability (EHSA) messages.
force-fail	Displays force failover messages.
image-download	Displays image download messages.
info-request	Displays information request messages.
nrp	Displays NRP messages.
ping	Displays ping messages.
status-update	Displays status update messages.
syslog	Displays PAM mailbox system log messages.
test1	Displays test1 messages.
test2	Displays test2 messages.
xc-request	Displays cross connect request messages.
xc-response	Displays cross connect response messages.

Defaults   No default behavior or values.

Command History

Release	Modification
12.1(4)DC	This command was introduced on the Cisco 6400 NRP-2.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples   This example shows how image download messages are received and transmitted by the PAM mailbox serial interface of the NRP-2 in slot 5. Notice that the request messages are 24 bytes long and the response messages are 12288 bytes long.

Switch# **debug pmbox rx-path tx-path image-download**

Switch#
RX(5/0) type:IMAGE DNLD, len = 24
TX(5/0) type:IMAGE DNLD, len = 12288
RX(5/0) type:IMAGE DNLD, len = 24
TX(5/0) type:IMAGE DNLD, len = 12288
RX(5/0) type:IMAGE DNLD, len = 24
TX(5/0) type:IMAGE DNLD, len = 12288

debug se64

To display debug messages for the NRP-2 ATM SAR, use the **debug se64** EXEC command. The **no** form of this command disables debugging output.

debug se64 {**detail** | **errors**}

no debug se64 {**detail** | **errors**}

Syntax Description		
detail	Enables the **show controllers atm 0/0/0** privileged EXEC command to display internal ATM SAR data and register values.	
errors	Displays run time SAR driver error information.	

Defaults   No default behavior or values.

Command History	Release	Modification
	12.1(4)DC	This command was introduced on the Cisco 6400 NRP-2.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

Examples   This debug output example shows that the SAR was not ready to transmit packets:

```
NRP-2# debug se64 errors

NRP-2#
01:39:05:%SYS-5-CONFIG_I:Configured from console by console
01:39:15:%NRP2_SE64-3-LLD_SNDPAK_SARNOTREADY:SAR not ready during packet TX:
vcd 2644
-Traceback= 60124A88 601CFF28 6012D878 602EFBCC 802C7EAC
01:39:45:%NRP2_SE64-3-LLD_SNDPAK_SARNOTREADY:SAR not ready during packet TX:
vcd 2249
-Traceback= 60124A88 601CFF28 6012D878 602EFBCC 802C7EAC
01:40:15:%NRP2_SE64-3-LLD_SNDPAK_SARNOTREADY:SAR not ready during packet TX:
vcd 3810
```

Related Commands	Command	Description
	show controllers atm 0/0/0	Displays information on the physical ATM interface.

debug vpdn pppoe-data

To display the contents of PPPoE session data packets, use the **debug vpdn pppoe-data** privileged EXEC command. Use the **no** form of the command to disable debugging output.

[**no**] **debug vpdn pppoe-data**

Syntax Description   This command has no arguments or keywords.

Defaults   Disabled

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples   The following type of output appears when a PPPoE data packet is transmitted by the router:

```
Jun 13 11:33:49.407: PPPoE: OUT
 contiguous pak, size 14
  FF 03 C0 21 02 0D 00 0A 05 06 1E 17 75 59
```

Related Commands

Command	Description
debug vpdn pppoe-errors	Displays PPPoE protocol and code errors.
debug vpdn pppoe-events	Displays PPPoE session events and incoming and outgoing active discovery packets.
debug vpdn pppoe-packets	Displays contents of PPPoE active discovery packets.

debug vpdn pppoe-errors

To display PPPoE protocol and code errors, use the **debug vpdn pppoe-errors** privileged EXEC command. Use the no form of the command to disable debugging output.

[**no**] **debug vpdn pppoe-errors**

Syntax Description   This command has no arguments or keywords.

Defaults   Disabled

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples   This example shows output from a PPPoE encounter with a MAC addressing error:

Jun 13 11:33:49.407: PPPoE: Bad MAC address: 1111.2222.3333

Related Commands

Command	Description
debug vpdn pppoe-data	Displays the contents of PPPoE session data packets.
debug vpdn pppoe-events	Displays PPPoE session events and incoming and outgoing active discovery packets.
debug vpdn pppoe-packets	Displays contents of PPPoE active discovery packets.

debug vpdn pppoe-events

To display PPPoE session events and incoming and outgoing active discovery packets, use the **debug vpdn pppoe-events** privileged EXEC command. Use the no form of the command to disable debugging output.

[**no**] **debug vpdn pppoe-events**

Syntax Description   This command has no arguments or keywords.

Defaults   Disabled

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples   The following display shows output when PPPoE established a virtual private networking session.

Jun 13 11:33:49.407: PPPOE: VPN session created.

Related Commands

Command	Description
debug vpdn pppoe-data	Displays the contents of PPPoE session data packets.
debug vpdn pppoe-errors	Displays PPPoE protocol and code errors.
debug vpdn pppoe-packets	Displays contents of PPPoE active discovery packets.

debug vpdn pppoe-packets

To display contents of PPPoE active discovery packets, use the **debug vpdn pppoe-packets** privileged EXEC command. Use the no form of the command to disable debugging output.

[**no**] **debug vpdn pppoe-packets**

Syntax Description   This command has no arguments or keywords.

Defaults   Disabled

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples   This example shows output from a PPPoE encounter with an active discovery packet.

```
Jun 13 11:33:49.407: PPPoE: discovery packet
 contiguous pak, size 74
  00 04 09 00 AA AA 03 00 80 C2 00 07 00 00 00 00
  22 22 33 33 00 50 73 27 5D C3 88 63 11 65 00 01
  00 1C 01 01 00 00 00 01 02 00 0A 70 70 70 6F 65 00
  .....
```

Related Commands

Command	Description
debug vpdn pppoe-data	Displays the contents of PPPoE session data packets.
debug vpdn pppoe-errors	Displays PPPoE protocol and code errors.
debug vpdn pppoe-events	Displays PPPoE session events and incoming and outgoing active discovery packets.

encapsulation aal5autoppp virtual-template

The PPP Autosense feature enables the NAS to distinguish between incoming PPPoA and PPPoE sessions and allocates resources on demand for both PPP types.

To enable PPP Autosense, use the **encapsulation aal5autoppp virtual-template** ATM VC or VC class command. To disable PPP Autosense, use the **no** form of this command.

> **encapsulation aal5autoppp virtual-template** *template-number*

> **no encapsulation aal5autoppp virtual-template** *template-number*

Syntax Description

template-number	Number of the virtual template that will be used to clone virtual-access interfaces for PPPoA sessions.

Defaults   Disabled

Command Modes   ATM VC or VC class

Command History

Release	Modification
12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   This command functions only when the PPPoA sessions are LLC encapsulated.

Do not use this command on a router that initiates PPPoA sessions.

Examples   This example shows how to enable PPP Autosense for virtual-template 1:

```
encapsulation aal5autoppp virtual-template 1
```

Related Commands

Command	Description
virtual-template pre-clone	Specifies the number of virtual access interfaces to be created and cloned from a specific virtual template.

initiate-to

To specify the IP address that will be tunneled to, use the **initiate-to** VPDN group command. To remove an IP address from the VPDN group, use the **no** form of this command.

initiate-to ip *ip-address* [**limit** *limit-number*] [**priority** *priority-number*]

no initiate-to [**ip** *ip-address*]

Syntax Description		
ip *ip-address*	IP address of the router that will be tunneled to.
limit *limit-number*	(Optional) Maximum number of sessions in each tunnel to the IP address.
priority *priority-number*	(Optional) Priority for the IP address (1 is the highest).

Defaults   Disabled.

Unlimited number of sessions per tunnel.

Command Modes   VPDN Group Mode

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.1(1) DC1	This command was modified for the Cisco 6400 NRP. The command option "**limit** *limit-number*" was extended for use without RPM, and its syntax description was modified. Sessions are now limited per tunnel instead of limited per IP address.

Usage Guidelines   Before you can use this command, you must enable one of the two request VPDN subgroups by using either the **request dialin** or **request dialout** command.

A LAC configured to request dial-in can be configured with multiple **initiate-to** commands to tunnel to more than one IP address.

An LNS configured to request dialout can only be configured with a single **initiate-to** command. If you enter a second **initiate-to** command, it will replace the original **initiate-to** command.

At least one **initiate-to** command must be configured for the VPDN group initiator services (**request-dialin** and **request-dialout**) to function.

Examples   This example shows how to configure VPDN group 1 to request up to three L2TP tunnels to the LNS. This group can tunnel a maximum of 40 sessions per tunnel.

```
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain net.com
 initiate-to ip 10.1.1.1 limit 40
 initiate-to ip 10.2.2.2 limit 40
 initiate-to ip 10.2.2.2 limit 40
!
```

Related Commands

Command	Description
request-dialin	Enables a router to request L2TP tunnels for dial-in.
request-dialout	Enables a router to request L2TP tunnels for dialout calls.

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 defining the start of the group.
end-IP	IP address defining the end of the contiguous addresses in the group.
group	Define a group containing 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 created without the optional **group** keyword is a member of the base system group.

Command Modes   Global configuration

Command History

Release	Modification
11.0	This command was introduced.
11.3AA	This command was enhanced to allow address ranges to be added and removed.
12.0	This command was migrated to Release 12.0.
12.1(5)DC	This command was modified for the Cisco 6400 NRP for the IP Overlapping Address Pools feature.

Usage Guidelines   All pool names must be unique. Use of a duplicate name simply extends that pool.

Specifying a (named) pool within a group allows their IP addresses to overlap those of pools in other groups and pools in the "base system" pool. However, (named) pool IP addresses cannot overlap within the same group. Belonging to a group does not otherwise affect processing of pools. This means that you can use (named) pools anywhere you can use pools.

Addresses are returned 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.

    ip local pool p1_g1 10.1.1.1 10.1.1.50 group grp1
    ip local pool p2_g1 10.1.1.100 10.1.1.110 group grp1
    ip local pool p1_g2 10.1.1.1 10.1.1.40 group grp2
    ip local pool lp1 10.1.1.1 10.1.1.10
    ip local pool p3_g1 10.1.2.1 10.1.2.30 group grp1
    ip local pool p2_g2 10.1.1.50 10.1.1.70 group grp2
    ip local pool lp2 10.1.2.1 10.1.2.10

This example specifies pool group "grp1" consisting of pools "p1_g1", "p2_g1" and "p3_g1"; pool group "grp2" consisting of pools "p1_g2", "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 may be an operational convenience, there is no required relationship 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.

l2tp tunnel receive-window

To set the local control channel receive window size (RWS), use the **l2tp tunnel receive-window** VPDN group command.

> **l2tp tunnel receive-window** *packets*

Syntax Description

packets	Specifies size, in packets, of local RWS.

Defaults
The default local RWS is platform dependent. For the Cisco 6400 NRP, the local RWS is 3000 packets.

Command Modes
VPDN group mode

Command History

Release	Modification
12.0(7) DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines
The local RWS determines the number of L2TP control packets that can be queued by the system for processing, and the new default local RWS is considerably larger than the value outlined in RFC 2661. While a large RWS enables the system to open PPP sessions more quickly, a small RWS is useful on networks that cannot handle large bursts of traffic.

Examples
This example shows how to set the local RWS to 500 packets:

```
l2tp tunnel receive-window 500
```

l2tp tunnel retransmit

To set the control channel retransmission parameters, use the **l2tp tunnel retransmit** VPDN group command. To disable a parameter setting, use the **no** form of this command.

l2tp tunnel retransmit [**retries** *value* | [**timeout** [**min** | **max**] *seconds*]]

no l2tp tunnel retransmit [**retries** *value* | [**timeout** [**min** | **max**] *seconds*]]

Syntax Description

retries	Retransmission attempts.
value	Specifies number of retransmission attempts.
timeout	Length of time between retransmission attempts.
min	Sets the minimum timeout.
max	Sets the maximum timeout, up to 8 seconds.
seconds	Specifies timeout length, in seconds.

Defaults

10 retries.

1-second timeout minimum.

8-second timeout maximum.

Command Modes

VPDN group mode

Command History

Release	Modification
12.0(7) DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines

Control channel retransmissions follow an exponential backoff, starting at the minimum retransmit timeout length, and ending at the maximum retransmit timeout length (up to 8 seconds). For example, if the minimum timeout length is set to 1 second, the next retransmission attempt occurs 2 seconds later. The following attempt occurs 4 seconds later, and all additional attempts occur in 8-second intervals.

Examples

This example shows how to configure 8 retransmission attempts, with the minimum timeout length set at 2 seconds and the maximum timeout length set at 4 seconds:

```
l2tp tunnel retransmit retries 8
l2tp tunnel retransmit timeout min 2
l2tp tunnel retransmit timeout max 4
```

Cisco 6400 Command Reference

lcp max-load-metric

To limit load metric, use the **lcp max-load-metric** global configuration command. To disable this limit, use the **no** form of the command.

lcp max-load-metric *number*

no lcp max-load-metric

Syntax Description

number	Maximum load metric based on the length of the PPP manager process input queue.

Defaults

Unlimited

Command Modes

Global configuration

Command History

Release	Modification
12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines

The nominal limit depends on many factors. Try several numbers and select the one that results in the shortest session recovery time after a link dropout.

Examples

This example shows how to limit the load metric to 100:

lcp max-load-metric 100

lcp max-session-starts

To limit the number of simultaneous link control protocol (LCP) session initiations, use the **lcpmax-session-starts** global configuration command. To disable this limit, use the **no** form of the command.

lcp max-session-starts *number*

no lcp max-session-starts

Syntax Description		
	number	Maximum number of simultaneous LCP session initiations.

Defaults   Unlimited number of simultaneous LCP sessions initiations

Command Modes   Global configuration

Command History

Release	Modification
12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   Range of possible values: 100 to 3000.

The nominal limit depends on many factors. Try several numbers and select the one that results in the shortest session recovery time after a link dropout.

Examples   This example shows how to limit the number of simultaneous LCP session initiations to 100:

lcp max-session-starts 100

local-profile

To configure a local service profile and enter profile configuration mode, use the **local-profile** global configuration command. Use the **no** form of this command to delete the local service profile.

local-profile *profile-name*

no local-profile *profile-name*

Syntax Description

profile-name	Name of profile to be configured.

Defaults   No default behavior or values.

Command Modes   Global configuration

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   Use this command to configure local service profiles.

Examples   The following example shows how to configure a RADIUS profile called cisco.com and enter profile configuration mode:

```
Router(config)# local-profile cisco.com
Router(config-prof)#
```

Related Commands

Command	Description
attribute	Configures attributes in local RADIUS profiles.
ssg service-search-order	Specifies the order in which NRP-SSG searches for a service profile.
show ssg open-garden	Displays a list of all configured open garden services.
ssg open-garden	Designates a service, defined in a local service profile, to be an open garden service.

multihop hostname

To enable the L2TP tunnel switch to initiate a tunnel based on the LAC host name or ingress tunnel ID, use the **multihop hostname** VPDN request-dialin group configuration mode command. To disable this option, use the **no** form of this command.

multihop hostname *ingress-tunnel-name*

no multihop hostname *ingress-tunnel-name*

Syntax Description

ingress-tunnel-name	LAC hostname or ingress tunnel ID.

Defaults   No default behavior or values.

Command Modes   VPDN request-dialin group

Command History

Release	Modification
12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples   This example shows how to enable the L2TP tunnel switch to forward sessions from LAC-1 through an outgoing tunnel to IP address 10.3.3.3:

```
!
vpdn-group 11
 request-dialin
  protocol l2tp
  multihop hostname LAC-1
 initiate-to ip 10.3.3.3
 local name Tunnel-Switch
!
```

Related Commands

Command	Description
domain *domain-name*	Selects VPDN group for tunnel initiation based on domain name.
dnis *dnis-number*	Selects VPDN group for tunnel initiation based on DNIS.

ppp ipcp mask

To request or reject IPCP subnet mask negotiation, or to specify a secondary subnet mask to use in case the RADIUS user profile does not contain one, use the **ppp ipcp mask** interface configuration command. To return to the default behavior, use the **no** form of this command.

ppp ipcp mask {*subnet-mask* / **reject** | **request** }

no ppp ipcp mask [*subnet-mask* | **reject** | **request**]

Syntax Description

subnet-mask	*a.b.c.d*—Subnet mask sent to requesting peer when the RADIUS user profile does not include the Framed-IP-netmask attribute.
reject	Rejects IPCP subnet mask negotiations.
request	Requests the subnet mask from the peer.

Defaults   Responds to IPCP subnet mask requests, but does not initiate IPCP subnet mask negotiations.

Command Modes   Interface configuration

Command History

Release	Modification
12.1(3) DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   Typically, the CPE is configured or hard coded to **request** the subnet mask information from the Cisco6400 NRP.

If the subnet mask is not available from either the NRP configuration or the RADIUS user profile, the NRP rejects the CPE request as if the **ppp ipcp mask reject** command was configured on the NRP.

Examples   In this example, the PPP sessions in PVC 1/43 are configured to support IPCP subnet negotiation. If the RADIUS user profile does not contain the Framed-IP-netmask attribute, the NRP returns 255.255.255.224 to the requesting CPE.

```
!
interface ATM 0/0/0.30 multipoint
 pvc 1/43
  encapsulation aal5ciscoppp Virtual-Template 2
 !
!
interface Virtual-Template 2
 ip unnumbered FastEthernet 0/0/0
 no peer default ip address
 ppp authentication pap chap
 ppp ipcp mask 255.255.255.224
```

ppp timeout authentication

To set the time to wait for a response from the remote peer before retransmitting a PAP authenticate request, CHAP challenge, or CHAP response, use the **ppp timeout authentication** interface configuration command. To return to the default timeout, use the **no** form of the command.

ppp timeout authentication *seconds*

no ppp timeout authentication

Syntax Description

seconds	0 - 255. Time between retransmissions.

Defaults   10 seconds

Command Modes   Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.1(1)DC	This command was first supported on the Cisco 6400 NRP for session scalability enhancements.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines   The nominal value depends on many factors. Cisco recommends that you start with a PPP authentication timeout of 15 seconds. Try several values and select the one that results in the highest number of stable sessions.

Examples   This example shows how to set authentication timeout to 15 seconds:

```
!
interface Virtual-Template1
 no ip address
 no logging event link-status
 keepalive 200
 no peer default ip address
 ppp authentication chap
 ppp timeout retry 15
 ppp timeout authentication 15
!
```

ppp timeout retry

To set the time the PPP state machine (for LCP and NCP) waits for a response from the remote peer before retransmitting a configuration request or connection termination request, use the **ppptimeout retry** interface configuration command. To return to the default timeout, use the **no** form of the command.

> **ppp timeout retry** *seconds*

> **no ppp timeout retry**

Syntax Description

seconds	1 - 255. Time between retransmissions.

Defaults   2 seconds

Command Modes   Interface configuration

Command History

Release	Modification
11.3	This command was introduced as **ppp restart-timer**.
12.2	This command was changed to **ppp timeout retry**.
12.1(1)DC	This command was modified for the Cisco 6400 NRP with a default of 2 seconds.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines   The nominal value depends on many factors. Cisco recommends that you start with a PPP retry timeout of 15 seconds. Try several values and select the one that results in the highest number of stable sessions.

Examples   This example shows how to set the retry timeout to 15 seconds:

```
!
interface Virtual-Template1
 no ip address
 no logging event link-status
 keepalive 200
 no peer default ip address
 ppp authentication chap
 ppp timeout retry 15
 ppp timeout authentication 15
!
```

pppoe limit max-sessions

To set the maximum number of PPP over Ethernet (PPPoE) sessions that are permitted on a router, and to set the PPPoE session count threshold at which an SNMP trap is generated, use the **pppoe limit max-sessions** command in virtual private dial-up network (VPDN) group configuration mode. To remove these settings, use the **no** form of this command.

    pppoe limit max-sessions *number-of-sessions* [**threshold-sessions** *threshold-value*]

    no pppoe limit max-sessions

Syntax Description		
	number-of-sessions	Maximum number of PPPoE sessions that will be permitted on the router. The range is from 0 to the maximum number of interfaces on the router.
	threshold-sessions	(Optional) Sets the PPPoE session limit threshold at which an SNMP trap is generated.
	threshold-value	Number of PPPoE sessions that will cause an SNMP trap to be generated. The range is from 0 to the maximum number of interfaces on the router.

Defaults
There is no default *number-of-sessions.*

The default *threshold-value* is the configured *number-of-sessions.*

Command Modes
VPDN group configuration

Command History	Release	Modification
	12.2(2)T	This command was introduced.
	12.2(7)T	This command was modified to configure the PPPoE session limit threshold.
	12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines
You must configure the **snmp-server enable traps pppoe** command in order for SNMP traps to be generated when the PPPoE session limit threshold is exceeded.

The following statements describe the different types of PPPoE session limits:

- The **pppoe limit max-sessions** command limits the total number of PPPoE sessions on the router, regardless of the type of medium the sessions are using.

- The **pppoe limit per-mac** command limits the number of PPPoE sessions that can be sourced from a single MAC address. This limit also applies to all PPPoE sessions on the router.

- The **pppoe limit per-vc** and **pppoe limit per-vlan** commands limit the number of PPPoE sessions on all PVCs or VLANs on the router. The **pppoe max-sessions** command limits the number of PPPoE sessions on a specific PVC or VLAN. Limits created for a specific PVC or VLAN using the **pppoe max-session** command take precedence over the global limits created with the **pppoe limit per-vc** and **pppoe limit per-vlan** commands.

Examples   The following example shows a limit of 100 PPPoE sessions configured for the router. An SNMP trap is generated when the number of PPPoE sessions on the router exceeds 90.

```
vpdn enable
!
vpdn-group 1
accept dialin
 protocol pppoe
 virtual-template 1
pppoe limit max-sessions 100 threshold-sessions 90
```

Related Commands

Command	Description
debug vpdn pppoe-errors	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.
pppoe limit per-mac	Specifies the maximum number of PPPoE sessions to be sourced from a MAC address.
pppoe limit per-vc	Specifies the maximum number of PPPoE sessions permitted on all VCs.
pppoe limit per-vlan	Specifies the maximum number of PPPoE sessions permitted on a VLAN.
pppoe max-sessions	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session count threshold at which an SNMP trap will be generated.
snmp-server enable traps pppoe	Enables PPPoE session count SNMP notifications.

pppoe limit per-mac

To limit the number of PPPoE sessions that can originate from a single MAC address, use the **pppoe limit per-mac** command.

pppoe limit per-mac *number*

Syntax Description	*number* The maximum number of PPPoE sessions for a single MAC address.

Defaults   100

Command Modes   Global configuration

Command History

Release	Modification
12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples   This example shows how to place a limit of 5 PPPoE sessions per MAC address:

pppoe limit per-mac 5

Related Commands

Command	Description
pppoe limit per-vc	Limits the number of PPPoE sessions that can be established on a VC.

pppoe limit per-vc

To limit the number of PPPoE sessions that can be established on a VC, use the **pppoe limit per-vc** command.

pppoe limit per-vc *number*

Syntax Description	*number*	The maximum number of PPPoE sessions for a VC.

Defaults   100

Command Modes   Global configuration

Command History

Release	Modification
12.0(3)DC	This command was first introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples

This example shows how to place a limit of 50 PPPoE sessions per VC:

pppoe limit per-vc 50

Related Commands

Command	Description
pppoe limit per-mac	Limits the number of PPPoE sessions that can be established on a single MAC address.

pppoe max-sessions

To set the maximum number of PPP over Ethernet (PPPoE) sessions that will be permitted on an ATM permanent virtual circuit (PVC), PVC range, virtual circuit (VC) class, or VLAN, and to set the PPPoE session count threshold at which an SNMP trap will be generated, use the **pppoe max-sessions** command in the appropriate command mode. To remove this specification, use the **no** form of this command.

pppoe max-sessions *number-of-sessions* [**threshold-sessions** *threshold-value*]

no pppoe max-sessions

Syntax Description		
number-of-sessions	Maximum number of PPPoE sessions that are permitted.	
threshold-sessions	(Optional) Sets the PPPoE session limit threshold at which an SNMP trap is generated. This option is not available in Ethernet subinterface configuration mode.	
threshold-value	Number of PPPoE sessions that will cause an SNMP trap to be generated. This option is not available in Ethernet subinterface configuration mode.	

Defaults

The default *number-of-sessions* is 100.

The default *threshold-value* is the *number-of-sessions.*

Command Modes

Ethernet subinterface
Interface-ATM-VC configuration
VC-class configuration
ATM PVC range configuration
PVC-in-range configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(2)T	This command was modified to limit PPPoE sessions on ATM PVCs, PVC ranges, and VC classes.
12.2(7)T	This command was modified to configure the PPPoE session limit threshold.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines

Note   You can configure PPPoE session limit thresholds for PVCs, PVC ranges, and VC classes. You cannot configure PPPoE session limit thresholds for VLANs.

You must configure the **snmp-server enable traps pppoe** command in order for SNMP traps to be generated when the PPPoE session limit threshold is exceeded.

The following statements describe the different types of PPPoE session limits:

 • The **pppoe limit max-sessions** command limits the total number of PPPoE sessions on the router, regardless of the type of medium the sessions are using.

 • The **pppoe limit per-mac** command limits the number of PPPoE sessions that can be sourced from a single MAC address. This limit also applies to all PPPoE sessions on the router.

 • The **pppoe limit per-vc** and **pppoe limit per-vlan** commands limit the number of PPPoE sessions on all PVCs or VLANs on the router. The **pppoe max-sessions** command limits the number of PPPoE sessions on a specific PVC or VLAN. Limits created for a specific PVC or VLAN using the **pppoe max-session** command take precedence over the global limits created with the **pppoe limit per-vc** and **pppoe limit per-vlan** commands.

PPPoE session limits created on an ATM PVC take precedence over limits created in a VC class or ATM PVC range.

PPPoE session limits created in an ATM PVC range take precedence over limits created in a VC class.

Examples **VLAN Example**

The following example shows a maximum of 200 PPPoE sessions configured for an 802.1Q VLAN subinterface:

```
interface FastEthernet0/0.10
 encapsulation dot1Q 10
 pppoe enable
 pppoe max-session 200
```

ATM PVC Example

The following example shows a limit of 10 PPPoE sessions configured for the PVC. An SNMP trap will be generated when the number of PPPoE sessions on the router exceeds 8.

```
interface ATM1/0.102 multipoint
 pvc 3/304
  encapsulation aal5snap
  protocol pppoe
  pppoe max-sessions 10 threshold-sessions 8
```

VC Class Example

The following example shows a limit of 20 PPPoE sessions and a session count threshold of 15 sessions configured for the VC class called "main":

```
vc-class atm main
 pppoe max-sessions 20 threshold-sessions 15
```

ATM PVC Range Example

The following example shows a limit of 30 PPPoE sessions configured for the ATM PVC range called "range-1". The session count threshold is also 30 sessions because when the *threshold-value* has not been explicitly configured, it defaults to the *number-of-sessions* value.

```
interface atm 6/0.110 multipoint
 range range-1 pvc 100 4/199
  encapsulation aal5snap
  protocol ppp virtual-template 2
  pppoe max-sessions 30
```

Individual PVC Within a PVC Range Example

The following example shows a limit of 10 PPPoE sessions configured for "pvc1", which is part of the ATM PVC range called "range1". The PPPoE session count threshold is also 10 sessions.

```
interface atm 6/0.110 multipoint
 range range1 pvc 100 4/199
  pvc-in-range pvc1 3/104
   pppoe max-sessions 10
```

	Command	Description
Related Commands	**debug vpdn pppoe-errors**	Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.
	pppoe limit max-sessions	Sets the maximum number of PPP over Ethernet (PPPoE) sessions that will be permitted on a router, and sets the PPPoE session count threshold at which an SNMP trap will be generated.
	pppoe limit per-mac	Specifies the maximum number of PPPoE sessions to be sourced from a MAC address.
	pppoe limit per-vc	Specifies the maximum number of PPPoE sessions permitted on all VCs.
	pppoe limit per-vlan	Specifies the maximum number of PPPoE sessions permitted on a VLAN.
	snmp-server enable traps pppoe	Enables PPPoE session count SNMP notifications.

protocol

Use the **protocol** command in the appropriate command mode to do one or more of the following tasks:

- Configure a static map for an ATM PVC, SVC, or VC class.

- Enable Inverse ARP or Inverse ARP broadcasts on an ATM PVC by either configuring Inverse ARP directly on the PVC or in a VC class (applies to IP and IPX protocols only).

- Configure PPP over Ethernet for an ATM PVC or VC class.

- Override the virtual-template configuration inherited from VC classes for all PPP over Ethernet encapsulations.

Use the **no** form of this command to remove a static map, disable Inverse ARP, or remove PPP over Ethernet encapsulation.

protocol *protocol* [*protocol-address* | **inarp**] [[**no**] **broadcast**] [**virtual-template** *number*]

no protocol *protocol* [*protocol-address* | **inarp**] [[**no**] **broadcast**] [**virtual-template** *number*]

Syntax Description	*protocol*	Choose one of the following keywords:
		aarp—AppleTalk ARP
		apollo—Apollo domain
		appletalk—AppleTalk
		arp—IP ARP
		bridge—bridging
		bstun—block serial tunnel
		cdp—Cisco Discovery Protocol
		clns—ISO CLNS
		clns_es—ISO CLNS end system
		clns_is—ISO CLNS intermediate system
		cmns—ISO CMNS
		compressedtcp—Compressed TCP
		decnet—DECnet
		decnet_node—DECnet node
		decnet_prime_router—DECnet prime router
		decnet_router-l1—DECnet router L1
		decnet_router-l2—DECnet router L2
		dlsw—data link switching
		ip—IP
		ipx—Novell IPX
		llc2—llc2
		pad—PAD links
		ppp—PPP over ATM LLC encapsulation
		pppoe—PPP over Ethernet encapsulation
		qllc—Qualified Logical Link Control protocol
		rsrb—remote source-route bridging
		snapshot—snapshot routing support
		stun—serial tunnel
		vines—Banyan VINES
		xns—Xerox Network Systems protocol
	protocol-address	Destination address that is being mapped to a PVC.
	inarp	(Only valid for IP and IPX protocols on PVCs) Use this keyword to enable Inverse ARP on an ATM PVC. If you specify a protocol-address instead of **inarp**, Inverse ARP is automatically disabled for that protocol.

Cisco 6400 Command Reference ■

[no] **broadcast**	(Optional) Broadcast indicates that this map entry is used when the corresponding protocol sends broadcast packets to the interface-. For example, IGRP updates. Pseudobroadcasting is supported. The broadcast keyword of the protocol command takes precedence if you previously configured the broadcast command on the ATM PVC or SVC.
virtual-template *number*	(Optional) Use these keywords and argument only when you specify pppoe encapsulation for the protocol argument. Specifies which virtual template number to use.

Defaults   Inverse ARP is enabled for IP and IPX if the protocol is running on the interface and no static map is configured.

Command Modes   Interface-ATM-VC configuration (for an ATM PVC or SVC)

VC-class configuration (for a VC class)

Command History

Release	Modification
11.3(3)T	This command was introduced.
12.0(3)DC	The **pppoe** keyword was added for the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   If the protocol command is not explicitly configured on an ATM PVC or SVC, the VC inherits the following default configuration (listed in order of next highest precedence):

- Configuration of the protocol command in a VC class assigned to the PVC or SVC itself.
- Configuration of the protocol command in a VC class assigned to the PVCs or SVCs ATM subinterface.
- Configuration of the protocol command in a VC class assigned to the PVCs or SVCs ATM main interface.
- Global default: Inverse ARP is enabled for IP and IPX if the protocol is running on the interface and no static map is configured.

Although you can assign an explicit network layer address to a virtual-template interface, Cisco recommends that you consider two other procedures. One procedure is to use AAA to assign an address to the virtual-access interface created from the virtual template, instead of configuring any network-layer address on the virtual template. The other procedure is to use an unnumbered IP address on the virtual template.

It is currently not possible to disable a virtual-access on an individual basis. To achieve a similar effect, either delete the relevant RADIUS user entries or deconfigure the VC associated with the virtual-access.

Examples   This example shows how to create a static map on a VC. 192.68.34.237 is connected to the VC and ATM pseudobroadcasts are sent.

protocol ip 192.68.34.237 broadcast

This example shows how to enable Inverse ARP for IPX. ATM pseudobroadcasts are not sent.

protocol ipx inarp no broadcast

This example shows how to remove a static map from a VC and restore the default behavior for Inverse ARP (refer to the "Default" section described above):

no protocol ip 192.68.34.237

This example shows how to configure PPP over Ethernet for an ATM PVC:

interface atm 2/0.1 multipoint
 pvc 0/60
  encapsulation aal5snap
  protocol pppoe

radius-server attribute 4 nrp

To change the default-selected IP address, use the **radius-server attribute 4 nrp** global configuration command. To restore the default-selected IP address, use the **no** form of this command.

radius-server attribute 4 nrp

no radius-server attribute 4 nrp

Syntax Description   This command has no arguments or keywords.

Defaults   The NSP IP address is sent in RADIUS attribute 4.

Command Modes   Global configuration mode

Command History

Release	Modification
12.1(5)DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   When using RADIUS attribute 4 and "format d" in a VPI/VCI configuration or in a SSG configuration, this command allows the default-selected IP address to be changed. This command can only be enabled if "format d" is already configured.

Table 1-1 shows how RADIUS global configuration commands can be combined to select an IP address.

Table 1-1   RADIUS Global Configuration Commands

Global Configuration Commands			Selected IP Address
ip radius source-interface <int *x*>	radius-server attribute nas-port format d	radius-server attribute 4 nrp	
Enabled			NRP IP Address [1]
	Enabled		NSP IP Address
Enabled	Enabled		NSP IP Address
Enabled	Enabled	Enabled	NRP IP Address [1]
	Enabled	Enabled	NRP best-select IP Address [2]

1. NRP IP Address of <int *x*>

2. Automatic choce, 1st choice is loopback, etc.

Examples   This example selects the NRP IP address to be sent in RADIUS attribute 4.

```
Router(config)# ip radius source-interface FastEthernet0/0/0
Router(config)# radius-server attribute nas-port format d
Router(config)# radius-server attribute 4 nrp
```

radius-server attribute 8 include in access-req

To send the IP address of a user to the RADIUS server in the access request, use the **radius-server attribute 8 include in access-req** global configuration command. To disable sending of the user IP address to the RADIUS server during authentication, use the **no** form of this command.

radius-server attribute 8 include in access-req

no radius-server attribute 8 include in access-req

Syntax Description   This command has no arguments or keywords.

Defaults   This feature is disabled.

Command Modes   Global configuration mode

Command History

Release	Modification
12.1(3)AA	This command was introduced on the Cisco AS5200, Cisco AS5300, and Cisco AS5800.
12.1(3)DC	This command was supported on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   Using the **radius-server attribute 8 include in access-req** command makes it possible for a network access server (NAS) to provide the RADIUS server with a hint of the user IP address in advance of user authentication. An application can be run on the RADIUS server to use this hint and build a table (map) of user names and addresses. By using the mapping information, service applications can begin preparing user login information to have available upon successful user authentication.

When a network device dials in to a NAS that is configured for RADIUS authentication, the NAS begins the process of contacting the RADIUS server in preparation for user authentication. Typically, the IP address of the dial-in host is not communicated to the RADIUS server until after successful user authentication. Communicating the device IP address to the server in the RADIUS access request allows other applications to begin to take advantage of that information.

As the NAS sets up communication with the RADIUS server, the NAS assigns an IP address to the dial-in host from a pool of IP addresses configured at the specific interface. The NAS sends the IP address of the dial-in host to the RADIUS server as attribute 8. At that time, the NAS sends other user information, such as the user name, to the RADIUS server.

After the RADIUS server receives the user information from the NAS, it has two options:

- If the user profile on the RADIUS server already includes attribute 8, the RADIUS server can override the IP address sent by the NAS with the IP address defined as attribute 8 in the user profile. The address defined in the user profile is returned to the NAS.

   • If the user profile does not include attribute 8, the RADIUS server can accept attribute 8 from the NAS.

The address returned by the RADIUS server is saved in memory on the NAS for the life of the session. If the NAS is configured for RADIUS accounting, the accounting start packet sent to the RADIUS server includes the same IP address as in attribute 8. All subsequent accounting packets, updates (if configured), and stop packets will also include the same IP address as in attribute 8.

Note   Configuring the NAS to send the host IP address in the RADIUS access request assumes that the login host is configured to request an IP address from the NAS server. It also assumes that the login host is configured to accept an IP address from the NAS. In addition, the NAS must be configured with a pool of network addresses at the interface supporting the login hosts.

Examples   This example shows a NAS configuration that sends the IP address of the dial-in host to the RADIUS server in the RADIUS access request. The NAS is configured for RADIUS authentication, authorization, and accounting (AAA). A pool of IP addresses (async1-pool) has been configured and applied at interface Async1.

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
ip address-pool local
!
interface Async1
 peer default ip address pool async1-pool
!
ip local pool async1-pool 10.165.200.225 10.165.200.229
!
radius-server host 10.31.71.146 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 8 include-in-access-req
radius-server key radhost
```

radius-server attribute nas-port format

To select the NAS port format used for RADIUS accounting features, use the **radius-serverattribute 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	Choose one of the following keywords:
	a—Standard NAS port format.
	b—Extended NAS port format.
	c—Shelf-slot NAS port format.
	d—ATM VC extended NAS port format.

Defaults

Standard NAS port format.

Command Modes

Global configuration mode

Command History

Release	Modification
11.3(7)T	This command was introduced.
11.3(9)DB and 12.0(5)DC	The **d** format was added for the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines

This command replaces the deprecated **radius-server attribute nas-port extended** command.

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).

- **Standard format (a)**—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 format (b)**—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 undergoing authentication.

- **Shelf-slot format (c)**—This 16-bit NAS port format supports expanded hardware models requiring shelf and slot entries.

- **ATM VC extended format (d)**—This NAS port format uses 32 bits to indicate the interface, VPI, and VCI of an incoming PPP session.

Note   The ATM VC extended NAS port format on the NRP applies only to VCs created or recreated after the command is entered. The format does not apply retroactively to VCs configured before the **radius-server attribute nas-port format d** command is entered.

Examples   This example shows how to select the ATM VC extended NAS port format used for RADIUS VCLogging:

radius-server attribute nas-port format d

Related Commands

Command	Purpose
radius-server host non-standard	Specifies a vendor-proprietary RADIUS server host.

snmp-server enable traps pppoe

To enable PPPoE session count Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps pppoe** global configuration command. To disable PPPoE session count SNMP notifications, use the **no** form of this command.

snmp-server enable traps pppoe

no snmp-server enable traps pppoe

Syntax Description	This command has no arguments or keywords.
Defaults	SNMP notifications are disabled by default.
Command Modes	Global configuration

Command History

Release	Modification
12.2(2)B	This command was introduced.
12.2(7)T	This command was integrated into Cisco IOS Release 12.2(7)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines

This command enables SNMP traps only. It does not support inform requests.

To configure the PPPoE session thresholds at which SNMP notifications will be sent, use the **pppoe limit max-sessions** or **pppoe max-sessions** commands.

For a complete description of this notification and additional MIB functions, see the CISCO-PPPOE-MIB.my file, available on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Examples

The following example enables the router to send PPPoE session count SNMP notifications to the host at the address 10.64.131.20:

```
snmp-server community public RW
snmp-server enable traps pppoe
snmp-server host 10.64.131.20 version 2c public udp-port 1717
```

Related Commands	Command	Description
	pppoe limit max-sessions	Sets the maximum number of PPP over Ethernet (PPPoE) sessions that will be permitted on a router, and sets the PPPoE session count threshold at which an SNMP trap will be generated.
	pppoe max-sessions	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session count threshold at which an SNMP trap will be generated.
	snmp-server host	Specifies the recipient of an SNMP notification operation.
	snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps atm pvc extension

To enable the sending of extended ATM permanent virtual circuit (PVC) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps atm pvc extension** global configuration command. To disable extended ATM PVC-specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps atm pvc extension {**up** | **down** | **oam failure loopback** }

no snmp-server enable traps atm pvc extension {**up** | **down** | **oam failure loopback** }

Syntax Description

up	Enables ATM PVC UP traps, which are generated when a PVC changes from the DOWN to UP state.
down	Enables ATM PVC DOWN traps, which are generated when a PVC changes from the UP to DOWN state.
oam failure loopback	Enables ATM PVC OAM FAILURE traps, which are generated when OAM loopback fails.

Defaults

SNMP notifications are disabled by default.

The interval between succesive traps is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced for those platforms that support ATM PVC Management.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines

You cannot use extended ATM PVC traps at the same time as the legacy ATM PVC trap. You must disable the legacy ATM PVC trap by using the **no snmp-server enable traps atm pvc** command before configuring extended ATM PVC traps.

When the ATM PVC OAM failure trap is enabled, the PVC remains in the UP state when OAM loopback fails so that the flow of data is still possible. If the ATM PVC OAM failure trap is not enabled, the PVC is placed in the DOWN state when OAM loopback fails.

OAM management must be enabled on the PVC by using the **oam-pvc manage** command before you can use ATM PVC traps.

Generation of PVC traps is dampened by the notification interval in order to prevent trap storms. No traps are sent until the interval lapses.

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. ATM notifications are defined in the CISCO-IETF-ATM2-PVCTRAP-MIB.my file, available from the Cisco FTP site:

ftp://www.cisco.com/public/mibs/v2/

ATM PVC traps are generated at the end of the notification interval. It is possible to generate all three types of ATM PVC traps (the ATM PVC DOWN trap, ATM PVC UP trap, and ATM PVC OAM failure trap) at the end of the same notification interval.

Use the **snmp-server enable traps atm pvc** command with the **snmp-server host** command.

Use the **snmp-server host** command to specify which hosts receive SNMP notifications. In order to send notifications, you must configure at least one **snmp-server host** command.

Examples   The following example shows all three extended ATM PVC traps enabled on a router. If PVC 0/1 leaves the UP or DOWN state, or has an OAM loopback failure, host 172.16.61.90 receives the SNMP notifications:

```
! Configure SNMP support and an IP routing protocol on your router:
Router(config)# snmp-server community public ro
Router(config)# snmp-server host 172.16.61.90 public
Router(config)# ip routing
Router(config)# router igrp 109
Router(config-router)# network 172.16.0.0
!
! Enable extended ATM PVC trap support and OAM management:
Router(config)# snmp-server enable traps atm pvc extension down
Router(config)# snmp-server enable traps atm pvc extension up
Router(config)# snmp-server enable traps atm pvc extension oam failure loopback
Router(config)# interface atm 1/0.1
Router(config-if)# pvc 0/1
Router(config-if-atm-vc)# oam-pvc manage
```

Related Commands

Command	Description
oam-pvc manage	Enables end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for an ATM PVC or VC class.
show atm pvc	Displays all ATM permanent virtual circuits (PVCs) and traffic information.
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server enable traps atm pvc	Enables the sending of legacy ATM PVC DOWN traps.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

tunnel share

To enable tunnel sharing for a VPDN group, use the **tunnel share** VPDN group command. To disable tunnel sharing, use the **no** form of this command.

tunnel share

no tunnel share

Syntax Description   This command has no arguments or keywords.

Defaults   Disabled.

Command Modes   VPDN group

Command History

Release	Modification
12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples   This example shows all sessions that are locally authorized through VPDN group 1 being sent through the same tunnel to 10.1.1.1.

```
!
vpdn-group 1
request-dialin
 protocol l2tp
 domain net1.com
 domain net2.com
initiate-to ip 10.1.1.1
tunnel share
!
```

Related Commands

Command	Description
vpdn-group	Selects the VPDN group.
request-dialin	Enables a router to request L2TP tunnels for dial-in.
initiate-to	Specifies the IP address that calls are tunneled to.

tx-ring-limit

To limit the number of particles that can be used on a transmission ring, use the **tx-ring-limit** ATM VC configuration command. To return to the default, use the **no** form of this command.

> **tx-ring-limit** *ring-limit*

> **no tx-ring-limit**

Syntax Description

ring-limit	Specifies the maximum number of allowable particles that can be placed on the transmission ring.

Defaults   2 particles on the Cisco 6400 NRP-2SV

Command Modes   This command is supported in the following command modes, numbered according to hierarchy:

1. ATM VC
2. PVC-in-range
3. PVC range
4. VC class
5. ATM interface

When you enter **tx-ring-limit** in a particular command mode, its value takes precedence over any value inherited from a command mode that is lower on the list.

Command History

Release	Modification
12.0(7)XE1	This command was introduced.
12.0(9)S	This command was integrated into Cisco IOS Release 12.0 S for the Cisco 7500/RSP series.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(2)B	This command was modified for the Cisco 6400 NRP-2SV:
	• New default of 2 particles
	• Added command to PVC range and PVC-in-range command modes
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   The **tx-ring-limit** command is not supported on the Cisco 6400 NRP-1.

The entered transmision ring limit is limited to values from 3 to 6000 particles.

On the Cisco 6400 NRP-2SV, the particle size is 2048 bytes.

What is a Transmissing Ring?

The transmission ring, a hardware first-in, first-out (FIFO) queue on the NRP-2SV ATM port adapter, stores packets before they are segmented into cells for transmission. When the queue is full, the NRP-2SV stops sending packets to the transmission ring and stores the packets in the Cisco IOS software until the transmission ring is no longer congested.

Choosing the Transmission Ring Limit

There is no ideal value for the transmission ring limit, so you must experiment to find the best value:

- A low transmission ring limit accelerates the traffic shaping performance in the IOS software and reduces latency for packets waiting to be segmented and transmitted. A lower transmission ring limit has a faster rate of dropped packets.

- A high transmission ring limit provides more buffering space and time for packets on that VC, but can cause performance problems for delay-sensitive traffic. A higher transmission ring limit has a slower rate of dropped packets.

Examples

In the following example, a transmission ring limit of seven particles is configured on the main ATM interface:

```
!
interface atm 0/0/0
 atm pvc 32 0 32 aal5snap 10000 8000 2000 tx-ring-limit 7
!
```

In the following example, a transmission ring limit of ten particles is configured directly on the PVC:

```
!
interface ATM0/0/0.1 point-to-point
 pvc 2/200
 tx-ring-limit 10
 !
```

In the following example, a transmission ring limit of five particles is configured for the PVC range from 6/32 to 6/4032:

```
!
interface atm 0/0/0
 range pvc 6/32 6/4032
 tx-ring-limit 5
!
```

In the following example, a transmission ring limit of six particles is configured for PVC 4/33 in the range 4/32 to 4/128:

```
!
interface atm 0/0/0
 range pvc 4/32 4/128
 !
 pvc-in-range 4/33
!
  tx-ring-limit 6
!
```

In the following example, a transmission ring limit of five particles is configured for VC class pppoa-1:

```
!
vc-class atm pppoa-1
 tx-ring-limit 5
!
```

Related Commands	Command	Description
	show atm vc	Displays information about ATM PVCs and SVCs.

virtual-template pre-clone

To specify the number of virtual-access interfaces to be created and cloned from a specific virtual template, use the **virtual-template pre-clone** global configuration command.

virtual-template *template-number* **pre-clone** *number*

Syntax Description	**virtual-template** *template-number*	The virtual template interface from which the new virtual-access interfaces are created.
	pre-clone *number*	The number of virtual-access interfaces created.

Defaults	None

Command Modes	Global configuration

Usage Guidelines   This command applies to PPPoE only.

The number of pre-cloned virtual-access interfaces should be set to the number of expected PPPoE sessions.

Command History	Release	Modification
	12.0(3)DC	This command was introduced on the Cisco 6400 NRP.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

Examples   This example shows how to create 1200 pre-cloned virtual-access interfaces on virtual template 1:

virtual-template 1 pre-clone 1200

vpdn authorize domain

To enable domain preauthorization on a NAS, use the **vpdn authorize domain** global configuration command. To disable domain preauthorization, use the **no** form of this command.

vpdn authorize domain

no vpdn authorize domain

Syntax Description   This command has no arguments or keywords.

Defaults   Domain preauthorization is disabled by default.

Command Modes   Global configuration

Command History

Release	Modification
12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples   This example shows how to enable domain preauthorization:

vpdn authorize domain

vpdn search-order

To specify how the service provider's network access server is to perform VPDN tunnel authorization searches, use the **vpdn search-order** global configuration command. To remove a prior specification, use the no form of the command.

> **vpdn search-order {dnis domain multihop-hostname}**

> **no vpdn search-order**

Syntax Description

multihop-hostname	Specifies a search on LAC host name or ingress tunnel ID.
domain	Specifies a search on the domain name.
dnis	Specifies a search on the DNIS information.

Defaults

The default vpdn search order is:

> **vpdn search-order** {**dnis domain**}

If authorization based on the multihop hostname is required, you will have to explicitly configure it as follows:

> **vpdn search-order** {**multihop-hostname dns domain**}

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.1(1) DC1	The **multihop-hostname** keyword was added for the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

VPDN authorization searches are performed only as specified.

The configuration shows the **vpdn search-order** command setting only if the command is explicitly configured.

Examples

This example shows how to configure an L2TP tunnel switch to perform each VPDN authorization search by the multihop-hostname, and if unsuccessful, search by the domain name.

vpdn search-order multihop-hostname domain

vpn service

To configure a static domain name, use the **vpn service** ATM VC or VC class configuration command. To remove a static domain name, use the **no** form of this command.

vpn service *domain-name*

no vpn service *domain-name*

Syntax Description

domain-name	Static domain name.

Defaults   No default behavior or values.

Command Modes   ATM VC or VC class

Command History

Release	Modification
12.1(1) DC1	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Examples   This example shows how to configure the static domain name of net.com:

vpn service net.com

vpn service

Show Commands for the Cisco 6400 NRP

This chapter describes the **show** commands that are specific to the Cisco 6400 node route processor (NRP).

Additional commands used to configure and monitor the Cisco 6400 NRP are described in:

• Chapter 1, "Commands for the Cisco 6400 NRP"

• Cisco IOS command reference publications available on Cisco.com or on the Cisco Documentation CD-ROM.

show atm ingress

To display the unique ingress VC information of local VCs, use the **show atm ingress** EXEC command.

show atm ingress [**all** | **local-vc** *vpi*/*vci*] [**detailed**]

Syntax Description

all	List the ingress VC info of all the local VCs.
local-vc	List the ingress VC info of a specific local VC.
vpi	Virtual path interface.
vci	Virtual circuit interface.
detailed	Print out detailed information for debugging.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(7) DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines

The information displayed using this command is used to construct NAS Port ID and NAS IP attributes in RADIUS authentication requests and accounting records when the global configuration command **radius attribute nas-port format d** is entered.

Examples

The following examples show the ingress local VC info:

```
Router# show atm ingress all
Local    VCD              Ingress   Ingress
Interface Name     VPI VCI Interface VPI/VCI    IPaddr
0/0/0.101 1        2   101  5/0/1    12/1001    10.20.30.40

0/0/0.102 2        2   102  5/0/1    12/1002    10.20.30.40

0/0/0.103 3        2   103  5/0/1    12/1003    10.20.30.40

Router# show atm ingress detailed
Local    VCD              Ingress   Ingress
Interface Name     VPI VCI Interface VPI/VCI    IPaddr
0/0/0.101 1        2   101  5/0/1    12/1001    10.20.30.40
    (0x611B5374/0x611B69EC/2/0xC20)
0/0/0.102 2        2   102  5/0/1    12/1002    10.20.30.40
    (0x611B7460/0x6120AA04/2/0xC24)
0/0/0.103 3        2   103  5/0/1    12/1003    10.20.30.40
    (0x6120BFD0/0x6120C584/2/0xC20)
```

Router# **show atm ingress local-vc 2/101**
Local:Interface:ATM0/0/0.101:VCD:1, VPI/VCI:2/101
Ingress:Interface:ATM5/0/1 VPI/VCI:12/1001 IP:10.20.30.40

Router# **show atm ingress local-vc 2/101 detailed**
Local:Interface:ATM0/0/0.101:VCD:1, VPI/VCI:2/101
Ingress:Interface:ATM5/0/1 VPI/VCI:12/1001 IP:10.20.30.40
    :0x611B5374/0x611B69EC Code:2 Flags:0xC20

Table2-1   **Show ATM Ingress** *Field Descriptions*

Field	Description
Local Interface	ATM interface or ATM subinterface (slot/subslot/port) viewed by the NRP
VCD or VCD Name	Virtual circuit descriptor
VPI	Virtual path interface
VCI	Virtual circuit interface
Ingress Interface	ATM interface (slot/subslot/port) viewed by the NSP
IP or IPaddr	IP address of the network management Ethernet port (NME) on the NSP
(*hexadecimal output*)	Diagnostic information

Related Commands

Command	Description
radius-server attribute nas-port format	Selects the NAS port format used for RADIUS accounting features.

show chassis xconn

To display the current state of the cross connect information requests from the NRP to the NSP, use the **show chassis xconn** EXEC mode command.

show chassis xconn

Syntax Description   This command has no keywords or arguments.

Defaults   No default behavior or values.

Command Modes   EXEC

Command History

Release	Modification
12.1(4)DC	This command was introduced on the Cisco 6400 NRP-2.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples   In the following example, there are no outstanding cross-connect requests from the NRP-2 to the NSP:

```
NRP-2> show chassis xconn
Xconn List len = 2048
 Req outstanding = 0, Req Pending = 0
 VC status
 ---------
 Outstanding_cnt = 0, Pending_cnt = 0
```

In the following example, one request is outstanding. The request is for PVC 40/50 on the NRP-2 ATM 0/0/0 interface. The request has nine more retries with a current timeout of 8000 milliseconds.

```
NRP-2# show chassis xconn
Xconn List len = 2048
 Req outstanding = 1, Req Pending = 0
 VC status
 ---------
 Outstanding VC (1002) 40/50, retry cnt = 9, timeout_period = 8000
 Outstanding_cnt = 1, Pending_cnt = 0
```

Related Commands

Command	Description
debug xconn	Displays debug NSP and NRP process cross-connect messages.

show controllers atm 0/0/0

To display information on the physical ATM interface of the Cisco 6400 NRP, use the **show controllers atm 0/0/0** privileged EXEC command.

Cisco 6400 NRP-2 or NRP-2SV

> **show controllers atm 0/0/0**

Cisco 6400 NRP-1

> **show controllers atm 0/0/0** [**detailed** | **scheduler** | **vc** *vpi/vci*]

Syntax Description	0/0/0	*slot/subslot/port* entry for the physical ATM interface of the Cisco 6400 NRP
	detailed	Output shows all available information
	scheduler	Output shows SAR scheduler information
	vc	Output shows information for the specified virtual circuit (VC)
	vpi/vci	Virtual path identifier (VPI) and virtual channel identifier (VCI) of the VC

Defaults

On the NRP-2 and NRP-2SV, the default output shows all available information on the ATM interface.

On the NRP-1, the default output shows only segmentation and reassembly (SAR) controller information.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2 GS	This command was introduced.
12.0(5)DA	This command was implemented on the Cisco 6260.
12.0(5)XE	This command was implemented on the Cisco 7200 and 7500 series routers.
12.0(5)T and 12.0(5)XK	This command was modified to support inverse multiplexing over ATM (IMA) groups on the Cisco 2600 and Cisco 3600 series routers.
12.0(7)XE1	This command was implemented on the Cisco 7100 series routers.
12.1(3)DC	This command was modified from its original version, with no display options, for the Cisco 6400 NRP-1: • To enable the output of cyclic redundancy check (CRC) error counts on a per-VC basis. • To display only SAR controller information as the default output. • With new options for controlling the output to include error counters on a per-VC basis.
12.1(4)DC	The command syntax was returned to its original form for the Cisco 6400 NRP-2.

Release	Modification
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples

In the following NRP-2 example, the output shows all available SAR controller information:

NRP-2# **show controllers atm 0/0/0**

*** SE64 General Data ***

Resources:

```
                 Thold  Thold  per-VC
 Pool   Total  Used  Free  Norm   Sys  Limit   VCs
------  -----  -----  -----  -----  -----  ------  -----
 TX-VBR  3273    1   3272  3241  3273  3273    1
 TX-UBR  409     8    401   377   409          2
 RX     32255    0  32255  21504  21568  3583   3
 MP-hld  49152   8   49144
```

Performance:

```
              Throttled  Throttled  Throttled  Spin
 Path  Total  Queued     Total      Sys   Hi Pri  avg/max
 ----  -----  ------  ----------  ----------  ----------  -------
 TX    3682     8        0          0        0   0/128
 RX    32255    0        0                        1/128
```

Other:
 TX hw Links = 2 RX Free (tbl) = 32255
 VPI/VCI bits = 3/11 SAR Rev = D

*** SE64 Global Statistics ***

RX Path:
 rx_giant_discard   = 0   rx_misc_discard   = 0
 rx_pkt   = 4   rx_drop_vc_bad   = 0
 rx_drop_crc   = 0   rx_drop_runt   = 0
 rx_drop_vc_del   = 0   rx_drop_giant   = 0
 rx_drop_throttle   = 0

RX OAM Path:
 rx_oam_spin_int   = 0   rx_oam_spin_poll   = 0
 rx_oam   = 0   rx_oam_drop_buf   = 0
 rx_oam_drop_crc_10 = 0

RX General:
 rx_count   = 0   rx_pkt_spin_start = 4
 rx_pkt_spin_total = 4   rx_spin_int   = 4
 rx_spin_poll   = 0   rx_pkt_clp   = 0
 rx_pkt_ci   = 0
TX Path:
 tx_pkt_safe_start = 8   tx_pkt_fast   = 0
 tx_drop_idb_down   = 0   tx_drop_vc_down   = 0
 tx_drop_vc_del   = 0   tx_drop_1par_clone = 0
 tx_drop_2par_room   = 0   tx_drop_2par_coal = 0
 tx_drop_gt2par   = 0   tx_drop_credit   = 0
 tx_drop_credit_sys = 0   tx_drop_credit_pri = 0
 tx_drop_oam_f4   = 0   tx_drop_pkt_len_0   = 0
 tx_drop_pkt_align   = 0   tx_drop_pkt_mp   = 0

TX General:

```
tx_count_vbr      = 0          tx_count_ubr       = 8
tx_tbl_count_vbr  = 1          tx_tbl_count_ubr   = 17
tx_vc_limit_vbr   = 3273       tx_pkt_spin_start  = 0
tx_pkt_spin_total = 0          tx_spin_int        = 0
tx_spin_poll      = 0          tx_combine         = 0
tx_2par_coal      = 0
```

```
SE64 stats interrupts:
 tx_desc_wm       = 0          tx_tmp_cb_full     = 0
 tx_cb_full       = 0          abr_sched_drift    = 0
```

```
SE64 error interrupts:
 rx_stat_rpt_ring_ful = 0          tx_stat_rpt_ring_ful = 0
 rm_cell_ring_full    = 0          rx_buf_pool1_mt      = 0
 rx_buf_pool2_mt      = 0          rx_buf_pool3_mt      = 0
 tx_buf_pkt_desc_mt   = 0          rx_cb_full           = 0
 rx_tmp_cb_full       = 0          fail_sched_abr_vc    = 0
 crm             = 0          biu_addr           = 0
 rx_cam_mult_hit = 0          tx_cam_mult_hit    = 0
 rx_hec          = 0          data_parity        = 0
```

In the following NRP-1 example, the output consists only of the SAR controller information:

```
NRP-1# show controllers atm 0/0/0
Interface ATM0/0/0
Hardware is ATM-SAR
PCI registers:
 bus_no=0, device_no=4
 CFID=0xA102104C, CFCS=0x02000006, CFRV=0x02030002, CFLT=0x0000FF00
 CFBA=0x4A000000, CFIT=0x02010100


*** TI1575 SAR at address 0x3A000000 ***
Receive/Transmit Statistics
 rx_isrs:    0        rx_isr_pkts: 1        rx_isr_bufs:  0
 rx_cells_ovf: 0        tx_cells_ovf: 0        hec_errors_ovf: 0
 rx_unkn_prot: 314        rx_aal5_disc: 0        rx_pkt_ovf:   0
 unkn_prot_ovf:0        aal5_disc_ovf: 0        tx_count:      0
 rx_crc_error: 0        rx_no_buf:   0        rx_timeout:    0
 rx_abort:   0        rx_cong_cells: 0        rx_freeze:     0
 rx_no_valbuf: 0        rx_bad_vc:   0        fallback act:  0
 tx_abort:   0        tx_no_desc:  0        tx_align:      0
 tx_freeze:  0        disabled:    0        enabled:       0
 tx_clones:  0        tx_xmt_paks: 3        teardown_vc:   0
 tx_pend_count_negative: 0
 tx_forced: 0        (0)
 tx_max_queued:    6144        seg_ring_size:    32
 tx output drops:    0
 pkt_too_big:      0        tx_pak_failed:    0
 idb_down:         0        invalid_pkt_type: 0
 invalid_vcd:      0        vc_ring_full:     0
 over_max_queued:  0        slot_owned_by_chip: 0
 vc_not_in_use:    0
 invalid_addr_count:  0


PCI Statistics
 detect_parity    0    system_error    0    master_abort    0
 rx_target_abort  0    sig_target_abort 0    data_parity     0


Internal registers
 config:   0x6037      status:  0x2000040 imask:    0xC381
 ratcount: 0x800       globrat: 0x79      rxunkn:   0x10000010
 txcompsize: 0x7FF     rxcompsize: 0x1FF      txsegsize: 0x1F
```

```
    aal5discard:0x0       hecerrors: 0x0       unknprot:  0x14C
    rxcells:  0x1       txcells:  0x1B       schedsize: 0x1
    txqueue:  0x80002009(spinerr:0) txpause:  0x0       chancount: 0x5
    txcompring: 0x311A00C  rxcompring: 0x3114020

    Structures common to all VCs
    receive free buffer ring
        address: 0x3110820  buf size: 10  ring size: 63  sar_indx: 1  drv_indx: 1
    receive completion ring
        addr: 0x3114000  indx: 1
    transmit completion ring
        addr: 0x311A000  indx: 3
```

In the following NRP-1 example, the output consists of all available information:

```
NRP-1# show controllers atm 0/0/0 detailed
Interface ATM0/0/0
Hardware is ATM-SAR
PCI registers:
 bus_no=0, device_no=4
 CFID=0xA102104C, CFCS=0x02000006, CFRV=0x02030002, CFLT=0x0000FF00
 CFBA=0x4A000000, CFIT=0x02010100


*** TI1575 SAR at address 0x3A000000 ***
Receive/Transmit Statistics
 rx_isrs:    0       rx_isr_pkts: 1       rx_isr_bufs:  0
 rx_cells_ovf: 0       tx_cells_ovf: 0       hec_errors_ovf: 0
 rx_unkn_prot: 514       rx_aal5_disc: 0       rx_pkt_ovf:   0
 unkn_prot_ovf:0       aal5_disc_ovf: 0       tx_count:     0
 rx_crc_error: 0       rx_no_buf:   0       rx_timeout:   0
 rx_abort:   0       rx_cong_cells: 0       rx_freeze:    0
 rx_no_valbuf: 0       rx_bad_vc:   0       fallback act:  0
 tx_abort:   0       tx_no_desc:  0       tx_align:     0
 tx_freeze:  0       disabled:   0       enabled:      0
 tx_clones:  0       tx_xmt_paks: 3       teardown_vc:  0
 tx_pend_count_negative: 0
 tx_forced: 0      (0)
 tx_max_queued:    6144      seg_ring_size:    32
 tx output drops:    0
 pkt_too_big:     0       tx_pak_failed:    0
 idb_down:       0       invalid_pkt_type:  0
 invalid_vcd:     0       vc_ring_full:     0
 over_max_queued:   0       slot_owned_by_chip: 0
 vc_not_in_use:    0
 invalid_addr_count:  0

PCI Statistics
 detect_parity   0   system_error   0   master_abort    0
 rx_target_abort  0   sig_target_abort 0   data_parity     0

Internal registers
 config:   0x6037     status:  0x2000040 imask:    0xC381
 ratcount: 0x800     globrat:  0x79     rxunkn:   0x10000010
 txcompsize: 0x7FF     rxcompsize: 0x1FF     txsegsize: 0x1F
 aal5discard:0x0       hecerrors: 0x0       unknprot:  0x214
 rxcells:  0x1       txcells:  0x1B       schedsize: 0x1
 txqueue:  0x80002009(spinerr:0) txpause:  0x0       chancount: 0x5
 txcompring: 0x311A00C  rxcompring: 0x3114020

 Structures common to all VCs
 receive free buffer ring
    address: 0x3110820  buf size: 10  ring size: 63  sar_indx: 1  drv_indx: 1
 receive completion ring
```

```
   addr: 0x3114000   indx: 1
transmit completion ring
   addr: 0x311A000   indx: 3

*** VC information and associated 1575 structures ***
seg ring: 5    ringaddr: 0x311C400  ringindx:0    pendindx:0
tx dma: 5    ctrlring: 0xC47100   pktcnt:   0
rword10:  0x0        rword11: 0x0
rword20:  0x0        rword21: 0x0        rword22: 0x0        rword23: 0x0
pxmt     0    queued:  0
 VCs mapped to this ring
 vcd:    1    cellhdr: 0x1E00640  encap:     0         crcerror: 0
  rx dma: 5    config: 0x24000000 ctrlrxring: 0x80000200  timecnt: 0xC8000
  lookup: 2    channel: 5        vpivci:    0x1E0064
seg ring: 6    ringaddr: 0x311C480  ringindx:0    pendindx:0
tx dma: 6    ctrlring: 0xC47120   pktcnt:   0
rword10:  0x0        rword11: 0x0
rword20:  0x0        rword21: 0x0        rword22: 0x0        rword23: 0x0
pxmt     0    queued:  0
 VCs mapped to this ring
 vcd:    2    cellhdr: 0x2800C80  encap:     0         crcerror: 0
  rx dma: 6    config: 0x24000000 ctrlrxring: 0x80000400  timecnt: 0xC8000
  lookup: 3    channel: 6        vpivci:    0x2800C8
seg ring: 7    ringaddr: 0x311C500  ringindx:0    pendindx:0
tx dma: 7    ctrlring: 0xC47140   pktcnt:   0
rword10:  0x0        rword11: 0x0
rword20:  0x0        rword21: 0x0        rword22: 0x0        rword23: 0x0
pxmt     0    queued:  0
 VCs mapped to this ring
 vcd:    3    cellhdr: 0xA0    encap:     0         crcerror: 0
  rx dma: 7    config: 0x24000000 ctrlrxring: 0x80000600  timecnt: 0xC8000
  lookup: 0    channel: 7        vpivci:    0xA
seg ring: 8    ringaddr: 0x311C580  ringindx:0    pendindx:0
tx dma: 8    ctrlring: 0xC47160   pktcnt:   0
rword10:  0x0        rword11: 0x0
rword20:  0x0        rword21: 0x0        rword22: 0x0        rword23: 0x0
pxmt     0    queued:  0
 VCs mapped to this ring
 vcd:    4    cellhdr: 0x500    encap:     0         crcerror: 0
  rx dma: 8    config: 0x24000000 ctrlrxring: 0x80000800  timecnt: 0xC8000
  lookup: 1    channel: 8        vpivci:    0x50
seg ring: 9    ringaddr: 0x311C600  ringindx:3    pendindx:3
tx dma: 9    ctrlring: 0xC47183   pktcnt:   0
rword10:  0x663C0000 rword11: 0x33CE274
rword20:  0x0        rword21: 0x33CDFC4 rword22: 0x0        rword23: 0x0
pxmt     0    queued:  0
 VCs mapped to this ring
 vcd:    5    cellhdr: 0x3200640  encap:     0         crcerror: 0
  rx dma: 9    config: 0x24000000 ctrlrxring: 0x80000A00  timecnt: 0xC8000
  lookup: 4    channel: 9        vpivci:    0x320064

*** TI1585/1585 Scheduler at address 0x3A040000 ***
Configuration/Statistics
 line bw:   149760   min vc bw: 64    total slots: 2
 free slots: 2

1585 internal registers
 config:   0x227      status:   0x1E       imask:    0x0
 clkfreq:  0x18FCA1   revnum:   0x0        acrlow:   0x80000000
 acrok:    0x80000000

1585 connection config/status
 scheduler id 5
    type: VBR     pcr: 353207   scr: 353207   mbs: 91
```

```
    rtv: 0x100
 scheduler id 6
    type: VBR       pcr: 353207   scr: 353207   mbs: 91
 rtv: 0x100
 scheduler id 7
    type: VBR       pcr: 353207   scr: 353207   mbs: 91
 rtv: 0x100
 scheduler id 8
    type: VBR       pcr: 353207   scr: 353207   mbs: 91
 rtv: 0x100
 scheduler id 9
    type: VBR       pcr: 353207   scr: 353207   mbs: 91
 rtv: 0x100
```

In the following NRP-1 example, the output consists of only the SAR scheduler information:

NRP-1# **show controllers atm 0/0/0 scheduler**
```
Interface ATM0/0/0
Hardware is ATM-SAR
PCI registers:
 bus_no=0, device_no=4
 CFID=0xA102104C, CFCS=0x02000006, CFRV=0x02030002, CFLT=0x0000FF00
 CFBA=0x4A000000, CFIT=0x02010100


 *** TI1585/1585 Scheduler at address 0x3A040000 ***
 Configuration/Statistics
 line bw:   149760   min vc bw: 64    total slots: 2
 free slots: 2

 1585 internal registers
  config:   0x227      status:   0x1E      imask:    0x0
  clkfreq:  0x18FCA1   revnum:   0x0       acrlow:   0x80000000
  acrok:    0x80000000

 1585 connection config/status
 scheduler id 5
    type: VBR       pcr: 353207   scr: 353207   mbs: 91
 rtv: 0x100
 scheduler id 6
    type: VBR       pcr: 353207   scr: 353207   mbs: 91
 rtv: 0x100
 scheduler id 7
    type: VBR       pcr: 353207   scr: 353207   mbs: 91
 rtv: 0x100
 scheduler id 8
    type: VBR       pcr: 353207   scr: 353207   mbs: 91
 rtv: 0x100
 scheduler id 9
    type: VBR       pcr: 353207   scr: 353207   mbs: 91
 rtv: 0x100
```

In the following NRP-1 example, the VC output consists only of information specific to VC 1/100:

NRP-1# **show controllers atm 0/0/0 vc 50/100**
```
Interface ATM0/0/0
Hardware is ATM-SAR
PCI registers:
 bus_no=0, device_no=4
 CFID=0xA102104C, CFCS=0x02000006, CFRV=0x02030002, CFLT=0x0000FF00
 CFBA=0x4A000000, CFIT=0x02010100


 *** VC information and associated 1575 structures ***
```

```
seg ring: 9    ringaddr: 0x311C600  ringindx:3    pendindx:3
tx dma: 9    ctrlring: 0xC47183  pktcnt:   0
rword10:  0x663C0000  rword11: 0x33CE274
rword20:  0x0      rword21: 0x33CDFC4  rword22: 0x0     rword23: 0x0
pxmt    0    queued:  0
VCs mapped to this ring
vcd:    5    cellhdr: 0x3200640  encap:    0       crcerror: 0
 rx dma: 9    config:  0x24000000 ctrlrxring: 0x80000A00  timecnt: 0xC8000
 lookup: 4    channel: 9      vpivci:   0x320064
```

In the following NRP-1 example, the output shows cyclic redundancy check (CRC) error counters for each configured VC:

```
NRP-1# show controllers atm 0/0/0 detailed | include crc
rx_crc_error: 0      rx_no_buf:  0      rx_timeout:   0
vcd:    1    cellhdr: 0x1E00640  encap:    0       crcerror: 0
vcd:    2    cellhdr: 0x2800C80  encap:    0       crcerror: 0
vcd:    3    cellhdr: 0xA0     encap:    0       crcerror: 0
vcd:    4    cellhdr: 0x500    encap:    0       crcerror: 0
vcd:    5    cellhdr: 0x3200640  encap:    0       crcerror: 0
```

Related Commands	Command	Description
	show se64 vc-stats	For the NRP-2, displays information for a specified VC.
	show atm interface	Displays ATM-specific information about an ATM interface.
	show atm pvc	Displays all ATM permanent virtual circuits (PVCs) and traffic information.
	show atm traffic	Displays current global ATM traffic information to and from all ATM networks connected to the router.
	show atm vc	Displays the ATM layer connection information about the virtual connections.
	debug se64 detail	Enables the **show controllers atm 0/00** command output to display internal ATM SAR data and register values.

show ip local pool

To display the local address pools, use the **show ip local pool** command.

show ip local pool [**group** *group-name* | [*poolname*]]

Syntax Description

group	define a group containing this pool
group-name	user-defined name for the pool group
pool-name	user-defined name for the local address pool

Defaults

If the group keyword is omitted, this command will show all local address pools.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.1(5)DC	This command was modified for the Cisco 6400 NRP to accommodate groups for the IP Overlapping Address Pools feature.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

None

Examples

The following example displays all pools:

```
router#sh ip local pool
Pool            Begin       End        Free  In use
** pool <p1> is in group <g1>
p1              10.1.1.1    10.1.1.10     10    0
                10.1.1.21   10.1.1.30     10    0
** pool <p2> is in group <g2>
p2              10.1.1.1    10.1.1.10     10    0
lcl1            20.2.2.1    20.2.2.10     10    0
                20.2.2.21   20.2.2.30     10    0
                20.2.2.41   20.2.2.50     10    0
** pool <mypool> is in group <mygroup>
mypool          172.18.184.223 172.18.184.224  2   0
                172.18.184.218 172.18.184.222  5   0
** pool <ccc> is in group <grp-c>
ccc             172.18.184.218 172.18.184.220  3   0
** pool <bbb> is in group <grp-b>
bbb             172.18.184.218 172.18.184.220  3   0
** pool <ddd> is in group <grp-d>
ddd             172.18.184.218 172.18.184.220  3   0
** pool <pp1> is in group <grp-pp>
pp1             172.18.184.218 172.18.184.220  2   1
```

The following example shows the pools in the group named mygroup:

```
router#sh ip local pool group mygroup
 Pool              Begin       End        Free  In use
 ** pool <mypool> is in group <mygroup>
 mypool            172.18.184.223  172.18.184.224    2     0
                   172.18.184.218  172.18.184.222    5     0
```

show nrp

To display the hardware configuration of the Cisco 6400 NRP, use the **show nrp** EXEC command.

show nrp

Syntax Description   This command has no keywords or arguments.

Command Modes   EXEC

Examples   The following is sample output from the **show nrp** command:

```
Router# show nrp
Router installed in slot 2

Network IO Interrupt Throttling:
 throttle count=0, timer count=0
 active=0, configured=0
 netint usec=4000, netint mask usec=200

NRP CPU ID EEPROM:
    Hardware revision 2.12        Board revision UNKNOWN (0xAF
    Serial number    4294967295   Part number    255-65535-255
    Test history    0xFF         RMA number    255-255-255
    EEPROM format version 0
    EEPROM contents (hex):
     0x00: 00 E3 02 0C FF FF FF FF FF FF FF FF FF FF FF FF
     0x10: FF FF FF FF FF FF FF FF FF FF FF 78 FF FF FF FF
```

show redundancy

To show which slots, subslots, ports, and CPUs are defined as redundant on the Cisco 6400, use the **show redundancy** command.

show redundancy [*slot*/*subslot*]

Syntax Description	*slot/subslot*	(Optional) Slot and subslot in chassis.

Command Modes   EXEC

Command History

Release	Modification
11.3(6)AA	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   The output of this command shows each object in a redundant pair and indicates which object is currently the master. Chassis redundancy appears if no slot or subslot is specified. If a slot or subslot is specified, the redundancy configuration for only that slot appears.

Examples   The following is sample output from the **show redundancy** command on the NRP:

```
Router# show redundancy

Primary   NRP in slot 2, system configured non redundant

User EHSA configuration (by CLI config):
slave-console = off
keepalive    = on
config-sync modes:
standard   = on
start-up  = on
boot-var  = on
config-reg = on

NSP EHSA configuration (via pam-mbox):
redundancy       = off
preferred (slot 2) = yes

Debug EHSA Information:
NRP specific information:
Backplane resets    = 0
NSP mastership changes = 0

print_pambox_config_buff: pmb_configG values:
valid        = 1
magic        = 0xEBDDBE1 (expected 0xEBDDBE1)
nmacaddrs      = 1
```

```
run_redundant   = 0x0
preferred_master = 0x1
macaddr[0][0]   = 0010.7b79.af93
macaddr[1][0]   = 0000.0000.0000

EHSA pins:
peer present = 0
peer state   = SANTA_EHSA_SECONDARY
crash status: this-nrp=NO_CRASH(1) peer-nrp=NO_CRASH(1)

EHSA related MAC addresses:
peer bpe mac-addr = 0010.7b79.af97
my   bpe mac-addr = 0010.7b79.af93
```

Related Commands	Command	Description
	show nrp	Displays the hardware configuration of the Cisco 6400 NRP.

show se64

To display detailed NRP-2 ATM SAR information, use the **show se64** EXEC command.

show se64 {**regs** | **mp_holder** | **vc-stats** *vpi vci* | **shaper** *shaper-number* | **vcd** *vcd*}

Syntax Description		
regs	Displays the values of internal registers for the NRP-2 ATM SAR.
mp_holder	Displays VCs with counters of outstanding SAR driver data structures used to recover transmitted packets. These data structures are referred to as "holders" or "mp holders."
vc-stats	Displays counters and statistics for a specific VC.
vpi vci	Virtual path identifier and virtual channel identifier.
shaper	Displays details of SAR driver data structures used to enforce traffic shaping specified by a VBR-NRT VC.
shaper-number	Shaper number. Valid values are 0 to 7.
vcd	Displays details of SAR driver data structures for a specific VC descriptor (VCD).
vcd	VC descriptor number. Valid values are 0 to 16383.

Defaults   No default behavior or values.

Command Modes   EXEC

Command History	Release	Modification
	12.1(4)DC	This command was introduced on the Cisco 6400 NRP-2.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   The **show se64** command is used for debugging and troubleshooting the NRP-2 ATM SAR.

The output of the **show se64 vc-stats** command is divided into five categories:

- General—Shows general statistics of the NRP-2 ATM SAR driver operation.

- RX Path—Shows statistics for the input and loss path of received packets through the NRP-2 ATM SAR driver, for the specified VC.

- RX General—Shows counters for the cells and packets received on the specified VC.

- TX Path—Shows statistics for the output and loss path of transmitted packets through the NRP-2 ATM SAR driver, for the specified VC.

- TX General—Shows counters for actions taken by the NRP-2 ATM SAR driver to successfully transmit certain packet types.

Note   The RX Path and TX Path output do not account for packets lost by the Cisco IOS.

Each shaper number can be mapped to one or more VCDs. The VCDs mapped to the selected shaper appears at the end of the **show se64 shaper** command output:

```
NRP-2# show se64 shaper 0
Shaper Number 0
pcr_kb 1000, pcr_cr 2271, pcr_count 24218
scr_kb 50, scr_cr 113, scr_count 4843600
mbs 10, mbs count 10
skip count 190, scr_inc 1023
VC on the shaper:
00002
```

To determine the VCD number to use in the **show se64 vcd** command, use the **show atm pvc** privileged EXEC command:

```
NRP-2# show atm pvc
          VCD /                     Peak  Avg/Min Burst
Interface Name    VPI VCI Type Encaps SC  Kbps  Kbps Cells Sts
0/0/0.100 1        0  300 PVC  SNAP   UBR 10000          UP
0/0/0.200 2        0  400 PVC  SNAP   VBR 1000   50   10 UP
0/0/0.300 foobe    0  500 PVC  SNAP   UBR 599040         UP
...
```

If the VCD is displayed as a name instead of a number for the PVC of interest, use the **showatmpvc** *name* privileged EXEC command to determine the VCD number:

```
NRP-2# show atm pvc foobe
ATM0/0/0.300:VCD:3, VPI:0, VCI:500, Connection Name:foobe
UBR, PeakRate:599040
AAL5-LLC/SNAP, etype:0x0, Flags:0xC20, VCmode:0x0
...
```

Examples

```
Router# show se64 regs
*** SE64 Internal Regs ***

SAR revision D


VPI bits 3, VCI bits 11


Number of free mp holders:49152
Number of particle in the sar 32255

rx buffer base:virtual 0C000000, physical AC000000
rx buffer size (byte):66058240, number of rx buffers:32255

OAM cell ring base:virtual 0B050000, physical AB050000
OAM shadow write pointer:0, OAM read pointer:10
OAM cell ring size (byte):65536, number of entries:1024

RM cell ring base:virtual 0AFC4000, physical AAFC4000
RM cell ring size (byte):16384, number of entries:256

Rx status ring base:virtual 0B020000, physical AB020000
Rx shadow write pointer:0, Rx read pointer:1284
Rx status ring size (byte):131072, number of entries:16384
```

Tx status ring base:virtual 0AFE0000, physical AAFE0000
Tx shadow write pointer:0, Tx read pointer:707
Tx status ring size (byte):131072, number of entries:16384

SE64 internal memory and registers base:virtual 24000000, physical 84000000
SE64 registers base:virtual 2401F000, physical 8401F000
SE64 local memory base:virtual 20000000, physical 80000000

Rx VC descriptor table base:virtual 20000000, physical 80000000
Rx VC descriptor table size(byte):1048576

Tx VC descriptor table base:virtual 20100000, physical 80100000
Tx VC descriptor table size(byte):1048576

Tx link pool base:virtual 20200000, physical 80200000
Tx link pool size(byte):794624
SE64 register value:
Addr 2401F000, high 84000037, low 84000037, Rc Lg Buffer Pool Config Register 1
Addr 2401F010, high FC000009, low FC000009, Rc Lg Buffer Pool Config Register 2
Addr 2401F020, high 7FF0000C, low 7FF0000C, Rc Sm Buffer Pool Config Register
Addr 2401F040, high 00000000, low 00000000, Rc Lg Buffer Pool Depth Register
Addr 2401F060, high 00000000, low 00000000, Rc Sm Buffer Pool Depth Register
Addr 2401F100, high 00000000, low 00000000, Rc Buffer Pool Return Register
Addr 2401F180, high 00000000, low 00000000, Rc Lg Buffer Pool Region Flag Regr
Addr 2401F190, high FFFFFFFF, low FFFFFFFF, Rc Sm Buffer Pool Row Map Regr 1
Addr 2401F1A0, high FFFFFFFF, low FFFFFFFF, Rc Sm Buffer Pool Row Map Regr 2
Addr 2401F400, high 00000090, low 00000090, Receive Processor Control Register
Addr 2401F410, high 00000000, low 00000000, Rc Ext. Descriptor Table Base Regr
Addr 2401F420, high 82FC4000, low 82FC4000, Rc RM Cell Ring Register
Addr 2401F430, high 83050285, low 83050285, Rc OAM Cell Ring Register
Addr 2401F440, high 80000000, low 80000000, Rc RM Cell Ring Stop Register
Addr 2401F450, high 8006800B, low 8006800B, Rc OAM Cell Ring Stop Register
Addr 2401F800, high 001C4FA7, low 00508002, Transmit Packet-Add Register 1
Addr 2401F808, high 00000000, low 82FC9038, Transmit Packet-Add Register 2
Addr 2401F810, high 11C28F06, low 11C28F06, Transmit Buffer-Add Register
Addr 2401F900, high 0000FEFE, low 0000FEFE, Tx Buf Link Pool Region FlagRegr
Addr 2401F908, high C0000001, low C0000001, Tx Buffer Link Pool Depth Register
Addr 2401FA00, high 00000000, low 00000000, Protocol Header Register 0H
Addr 2401FA08, high 00000000, low 00000000, Protocol Header Register 0L
Addr 2401FA10, high 00000000, low 00000000, Protocol Header Register 1H
Addr 2401FA18, high 00000000, low 00000000, Protocol Header Register 1L
Addr 2401FA20, high 00000000, low 00000000, Protocol Header Register 2H
Addr 2401FA28, high 00000000, low 00000000, Protocol Header Register 2L
Addr 2401FA30, high 00000000, low 00000000, Protocol Header Register 3H
Addr 2401FA38, high 00000000, low 00000000, Protocol Header Register 3L
Addr 2401FA40, high 00000000, low 00000000, Protocol Header Register 4H
Addr 2401FA48, high 00000000, low 00000000, Protocol Header Register 4L
Addr 2401FA50, high 00000000, low 00000000, Protocol Header Register 5H
Addr 2401FA58, high 00000000, low 00000000, Protocol Header Register 5L
Addr 2401FA60, high 00000000, low 00000000, Protocol Header Register 6H
Addr 2401FA68, high 00000000, low 00000000, Protocol Header Register 6L
Addr 2401FA70, high 00000000, low 00000000, Protocol Header Register 7H
Addr 2401FA78, high 00000000, low 00000000, Protocol Header Register 7L
Addr 2401FA80, high 00000000, low 00000000, Protocol Header Register 8H
Addr 2401FA88, high 00000000, low 00000000, Protocol Header Register 8L
Addr 2401FA90, high 00000000, low 00000000, Protocol Header Register 9H
Addr 2401FA98, high 00000000, low 00000000, Protocol Header Register 9L
Addr 2401FAA0, high 00000000, low 00000000, Protocol Header Register AH
Addr 2401FAA8, high 00000000, low 00000000, Protocol Header Register AL
Addr 2401FAB0, high 00000000, low 00000000, Protocol Header Register BH
Addr 2401FAB8, high 00000000, low 00000000, Protocol Header Register BL
Addr 2401FB00, high 00000000, low 00000000, VC Base Address Register
Addr 2401FB08, high 00FFFFFF, low 00FFFFFF, FRM Cell Time Interval Register
Addr 2401FB10, high 00000000, low 00000000, CRM Interrupt Register

...
(additional register settings deleted)
...

NRP-2# **show se64 mp_holder**
Number of free mp holders:49146

vcd 1, number of holders 6

Number of mp holders in the closed VC queue:0

NRP-2# **show se64 vc-stats 4 33**
*** SE64 Statistics for VPI/VCI = 4/33 ***

General:
 rx_count   = 0   rx_limit   = 7064
 tx_count   = 0   tx_limit   = 40

RX Path:
 rx_pkt   = 209   rx_drop_giant   = 0
 rx_drop_crc   = 7   rx_drop_runt   = 0
 rx_drop_vc_del   = 0   rx_drop_throttle = 0

RX general:
 rx_pkt_clp   = 0   rx_pkt_ci   = 0
 rx_cell_count   = 319

TX Path:
 tx_pkt_safe_start = 224   tx_pkt_fast   = 27
 tx_drop_idb_down = 0   tx_drop_vc_down   = 0
 tx_drop_vc_del   = 0   tx_drop_1par_clone = 0
 tx_drop_2par_room = 0   tx_drop_2par_coal = 0
 tx_drop_gt2par   = 0   tx_drop_credit   = 0
 tx_drop_oam_f4   = 0   tx_drop_pkt_len_0 = 0
 tx_drop_pkt_align = 0   tx_drop_pkt_mp   = 0

TX General:
 tx_combine   = 0   tx_2par_coal   = 0

NRP-2# **show se64 shaper 0**
Shaper Number 0
pcr_kb 1000, pcr_cr 2271, pcr_count 24218
scr_kb 50, scr_cr 113, scr_count 4843600
mbs 10, mbs count 10
skip count 190, scr_inc 1023
VC on the shaper:
00002

If the shaper has no PVCs assigned to it, the **show se64 shaper** command shows an invalid status:

NRP-2# **show se64 shaper 3**
Shaper Number 3
Status:Invalid

NRP-2# **show se64 vcd 1**
TX
Addr 20100000, high 9BD294BF low 00000001
Addr 20100008, high 0000001C low 98000000
Addr 20100010, high 00000000 low 0006000D
Addr 20100018, high 40000000 low 00000000
Addr 20100020, high 80000000 low 000012C0
Addr 20100028, high 00000000 low 00000000
Addr 20100030, high 00000000 low 00000000
Addr 20100038, high 00000000 low 00000000

```
RX
Addr 20004B00, high C704DD7B low 21000000
Addr 20004B08, high 00000002 low BC0010B0
Addr 20004B10, high 00000000 low 00000000
Addr 20004B18, high 00000000 low 00000000
Addr 20004B20, high 80001010 low 00000000
Addr 20004B28, high 00000000 low 00000000
Addr 20004B30, high 00000000 low 00000000
Addr 20004B38, high 00000000 low 00000000
```

Related Commands	Command	Description
	show controllers atm 0/0/0	Displays global (as opposed to VC-specific) information on the physical ATM interface.

show vtemplate

To display a list of all configured virtual templates, use the **show vtemplate** privileged EXEC command.

show vtemplate

Syntax Description   This command has no arguments or keywords.

Defaults   This command has no default behavior or values.

Command Modes   Privileged EXEC

Command History

Release	Modification
12.0(7) DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples   In the following example, precloning is on for Virtual-Template 1, 250 virtual access interfaces have been precloned, and 249 virtual access interfaces are available for new L2TP sessions. Only one virtual access interface is in use by L2TP, and no virtual access interfaces were cloned during call setup.

```
Router# show vtemplate
 Virtual-Template 1, pre-cloning is on
  Pre-clone limit: 250, current number: 249
  Active vaccess number: 1

 Generic free vaccess number:0
```

Table2-2 describes the fields shown in the example.

Table2-2   **Show Vtemplate** *Field Descriptions*

Field	Description
virtual template name	Configured interface name of virtual template.
pre-cloning is *on/off*	Indicates whether precloning is on or off for that virtual template.
Pre-clone limit	Number of precloned virtual access interfaces.
current number	Number of currently available precloned virtual access interfaces.
Active vaccess number	Number of virtual access interfaces in use.
Generic free vaccess number	Number of virtual access interfaces that were cloned at call setup (not precloned).

3

Commands for the Cisco 6400 NSP

This chapter describes the commands and tasks specific to the Cisco 6400 node switch processor (NSP) except for show commands, which are described in:

*   Chapter4, "Show Commands for the Cisco 6400 NSP"

*   *ATM and Layer 3 Switch Router Command Reference,* available at www.cisco.com or on the Cisco Documentation CD-ROM.

aps clear

To clear all of the APS priority requests created by the **aps signal-degrade, aps lockout, aps force, and aps manual** commands, use the **aps clear** EXEC command.

aps clear atm *slot/subslot/port*

Syntax Description

slot/subslot/port	Specifies the ATM interface for which you want all APS priority requests cleared.

Defaults

None

Command Modes

EXEC configuration

Usage Guidelines

This command applies to the Cisco 6400 NSP only.

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 if redundancy is configured on the specified interface.

Examples

In the following example, all the current APS priority requests on ATM 2/0/1 are cleared.

Switch# **aps clear atm 2/0/1**

Related Commands

aps force
aps lockout
aps manual

aps force

To force an interface to switch to the alternate port within a redundant pair, use the **aps force** EXEC command.

> **aps force atm** *slot*/*subslot*/*port* **from** [**protection** | **working**]

Syntax Description	*slot*/*subslot*/*port*	Specifies the interface you want to affect.

slot/*subslot*/*port*	Specifies the interface you want to affect.
from protection	Specifies that you want to switch from the protection port to the working port.
from working	Specifies that you want to switch from the working port to the protection port.

Defaults   None

Command Modes   EXEC mode

Usage Guidelines   This command applies to the Cisco 6400 NSP only.

Force is a defined APS request priority level. The request succeeds if no higher priority request (lockout is the only higher priority request) is posted. The **aps force** command does not persist over a system restart. The port type named in the command indicates the member of the redundant port pair that you want to switch away from.

For more information about APS priority requests, see the Telcordia GR-253-CORE specification.

> **Note**   This command works only if redundancy is configured on the specified interface.

Examples   The following example shows the ATM 1/1/1 interface being forced to switch from the working port to the protection port within the defined redundant pair.

Switch# **aps force atm 1/1/1 from working**

Related Commands   **aps clear**
aps lockout
aps manual

aps lockout

To lock out the protection port within a redundant pair, use the **aps lockout** EXEC command.

> **aps lockout atm** *slot/subslot/port*

Syntax Description

slot/subslot/port	Specifies the interface you want to affect.

Defaults   None

Command Modes   EXEC mode

Usage Guidelines   This command applies to the Cisco 6400 NSP only.

Lockout is defined as the highest APS request priority level. The **aps lockout** command does not persist over a system restart. When the protection port is locked out, only the working port is used for the specified interface.

For more information about APS priority requests, see the Telcordia GR-253-CORE specification.

> **Note**   This command works only if redundancy is configured on the specified interface.

Examples   In the following example, the ATM 1/1/1 interface is forced to use the working port within the defined redundant pair.

Switch# **aps lockout atm 1/1/1**

Related Commands   **aps clear**
aps force
aps manual

aps manual

To post an APS request that switches an interface to the alternate port within a redundant pair, use the **aps manual** EXEC command.

aps manual atm *slot/subslot/port* **from** [**protection** | **working**]

<table>
<tr><td>Syntax Description</td><td>*slot/subslot/port*</td><td>Specifies the interface you want to affect.</td></tr>
<tr><td></td><td>**from protection**</td><td>Specifies that you want to switch from the protection port to the working port.</td></tr>
<tr><td></td><td>**from working**</td><td>Specifies that you want to switch from the working port to the protection port.</td></tr>
</table>

Defaults   None

Command Modes   EXEC mode

Usage Guidelines   This command applies to the Cisco 6400 NSP only.

Manual is a defined 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 port type named in the command indicates the member of the redundant port pair that you want to switch away from.

Table 3-1 lists the priority requests, relevant to the Cisco 6400, that are higher than manual.

s

Table 3-1   APS Priority Request

Priority	Priority request
1	Lockout of protection
2	Forced switch
3	SF - Low priority
4	SD - Low priority
5	Manual switch

For a complete list of priority requests, see Table 5.3 of the Telcordia GR-253-CORE specification.

Note   This command works only if redundancy is configured on the specified interface.

Examples   In the following example, the ATM 1/1/1 interface is switched from the working port to the protection port within the defined redundant pair, provided that no higher priority request is posted.

Switch# **aps manual atm 1/1/1 from working**

Related Commands   aps clear
aps force
aps lockout

aps mode

To set the APS operational mode on a Cisco 6400 for a pair of redundant ports, use the **aps mode** interface command. To remove the APS operational mode, use the **no associate** command.

aps mode {**linear 1+1 nonreverting unidirectional**}

Syntax Description

linear 1+1 nonreverting unidirectional	Specifies that the APS operation between the two redundant ports for the interface is linear, 1+1, nonreverting, and unidirectional.

Defaults   On

Command Modes   Interface configuration

Usage Guidelines   This command applies to the Cisco 6400 NSP only.

The linear 1+1 nonreverting unidirectional mode is the only APS mode currently supported on the Cisco 6400.

There is only one logical interface for a pair of redundant ports. The APS configuration commands are accepted only on an interface that represents a redundant pair of ports. If the redundancy between ports is removed by using the **no associate** command, two interface configuration sections are created, but the APS configuration commands are removed from both.

Note   The APS mode is enabled by default on all Cisco 6400 OC-3 line cards.

The **aps mode** must be set before the other **aps** commands can be entered.

Examples   In the following example, the ATM interface 1/0/0 is configured for linear APS operation.

Switch(config)# **interface atm 1/0/0**
Switch(config-if)# **aps mode linear 1+1 nonreverting unidirectional**

Related Commands   **associate**

aps signal-degrade

To set the bit-error-rate threshold for signal degrade APS priority posting, use the **aps signal-degrade** interface configuration command. To remove the BER threshold, use the **no** form of this command.

aps signal-degrade BER threshold *value*

no aps signal-degrade BER threshold *value*

Syntax Description		
BER threshold	Specifies the name of the priority request for which you are setting a threshold.
value	Specifies the value of the threshold, which is 10-x, where x is 5, 6, 7, 8, or 9.

Defaults   None

Command Modes   Interface configuration

Usage Guidelines   This command applies to the Cisco 6400 NSP only.

For a complete list of priority requests, see Table 5.3 of the Telcordia GR-253-CORE specification.

Examples   In the following example, the BER threshold for the ATM 1/0/1 interface is set to 9.

```
Switch(config)# interface atm 1/0/1
Switch(config-if)# aps signal-degrade BER threshold 9
```

Related Commands   **aps signal-fail**
aps mode
snmp-server forwarder
show controllers

aps signal-fail

To set the bit-error-rate threshold for signal fail APS priority posting, use the **aps signal-fail** interface configuration command. To restore the default BER threshold, use the **no** form of this command.

aps signal-fail BER threshold *value*

no aps signal-fail BER threshold

Syntax Description	BER threshold	Specifies the name of the priority request for which you are setting a threshold.
	value	Specifies the value of the threshold, which is 10^{-x}, where x is 3, 4, or 5.

Defaults
The default BER threshold is 10^{-3}.

Command Modes
Interface configuration

Usage Guidelines
This command applies to the Cisco 6400 NSP only.

For a complete list of priority requests, see Table 5.3 of the Telcordia GR-253-CORE specification.

Examples
In the following example, the BER threshold for the ATM 1/0/1 interface is set to 5.

```
Switch(config)# interface atm 1/0/1
Switch(config-if)# aps signal-fail BER threshold 5
```

Related Commands
aps signal-degrade
aps mode
show aps
show controllers

archive tar

To list the contents of a UNIX-style tar archive or to extract its contents, use the **archive tar** privileged EXEC command.

archive tar /table *URL*

archive tar /xtract *source destination*

Syntax Description

/table	Lists the contents of the tar archive.
URL	Specifies the location of the tar archive you want to list.
/xtract	Extracts the contents of the source tar archive to the destination given.
source	Specifies the source of the tar file you want to extract.
destination	Specifies the destination of the tar file you want to extract. Usually installed from Flash disk on the NSP.

Defaults   None

Command Modes   Privileged EXEC

Usage Guidelines   This command applies to the Cisco 6400 NSP only.

This command is mostly used to unpack updated Web Console pages. The Cisco 6400 ships with current Web Console HTML pages; however, you should download new or updated pages from time to time. The new pages will be stored in a tar archive that you must unpack with the **archive tar** command before viewing.

Examples   The following example shows how to extract files on the TFTP server named *boothost* and install them on the disk located in slot 0 on the NSP:

Switch# **archive tar /xtract tftp://boothost/6400/c6400s-html.tar disk0:**

associate

To group two slots or two subslots for redundant operation, use the **associate** redundancy subcommand. To remove the redundancy, use the **no** form of this command.

associate {**slot** *slot* [*slot*] | **subslot** *slot/slubslot* [*slot/subslot*]}

no associate {**slot** *slot* [*slot*] | **subslot** *slot/slubslot* [*slot/subslot*]}

Syntax Description

slot	Specifies that redundancy is set between two slots.
subslot	Specifies that redundancy is set between two subslots.
slot *slot/subslot*	Specifies the slot or subslot for the member of a redundant pair. You do not need to specify the second member of the pair because only adjacent devices can be configured as redundant.

Defaults   No redundancy

Command Modes   Redundancy configuration

Usage Guidelines   This command can be entered only from the Cisco 6400 NSP.

The **associate** command must be entered in redundancy configuration mode. Redundant pairs consist of the odd-numbered slot and the following even-numbered slot. For example, slots 1 and 2 can be configured as a redundant pair but slots 2 and 3 cannot be configured as a redundant pair. The same applies to redundant subslots. For example, subslots 7/1 and 8/1 can form a redundant pair.

When you use the **associate** command for two slots, it implies that the related subslots are also associated and behave in a redundant manner.

Examples   In the following example, Cisco 6400 slots 1 and 2 are configured for redundant operation. You need only specify the first member of a redundant pair.

Switch(config)# **redundancy**
Switch(config-r)# **associate slot 1**

Related Commands   **redundancy**
show redundancy

atm input-xlate-table autominblock

To enable automatic determination of minimum Input Translation Table block sizes for all virtual path identifiers (VPI's) populated with permanent virtual circuits (PVC's) and Soft PVC source legs, use the **atm input-xlate-table autominblock** global configuration mode command. To disable autominblock mode, use the **no** form of this command.

atm input-xlate-table autominblock

no atm input-xlate-table autominblock

Syntax Description   This command has no arguments or keywords.

Defaults   Autominblock mode is disabled.

Command Modes   Global configuration mode

Command History

Release	Modification
12.1(4)DB	This command was introduced on the Cisco 6400 NSP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   When you enable the autominblock mode on a Node Switch Processor (NSP), the system analyzes all interfaces and determines minimum ITT block sizes for all VPIs populated with PVCs and Soft PVC source legs that can use the ITT (but a point to-multipoint leaf would not be included). The autominblock mode also updates the analysis when virtual circuits (VC's) are added or deleted. If you generate the configuration command-line interface (CLI), for example, by using the **more system:running-config** command, **minblock** commands are inserted as appropriate for all VPIs populated with PVCs on all external ATM interfaces.

You can specify a minimum block size for an interface and VPI combination by using the **force** keyword, even when the **autominblock** command is enabled. See the following table for the effect of **minblock** commands in different situations:

Enable autominblock command	Use force keyword	Effect
true	true	The *blocksize* value is not overridden by automatic analysis.
true	false	The *blocksize* value can be overridden by automatic analysis.
false	true	The command is accepted.
false	false	The command is not accepted.

Note Enabling the autominblock mode does not alter the usage state of ITT at the moment the command is invoked in a running system. Since ITT memory may have already been allocated, autominblock mode alters only the subsequent behavior of the system.

Similarly, autominblock mode does not eliminate fragmentation generated as a result of VCs configured after the autominblock mode is enabled, but ensures that the software allocates optimal-size blocks on interface flaps subsequent to the definition of a PVC with a maximum VCI.

To ensure that the software subsequently allocates optimal-sized ITT blocks—even after you restart the system—enable the autominblock mode before or after all PVCs are defined. Save the configuration by using the **copy running-config startup-config** command.

You do not need to set up a cross-connect to specify a minimum block through autominblock analysis. Because autominblock analysis considers PVC half legs, you can use these half legs to establish the maximum intended virtual channel identifier (VCI) range, which helps to eliminate the growth of ITT block sizes in the future.

Note When the initial attempt to allocate an ITT block fails and the actual size needed is less than the specified minimum block size, the software retries the allocation by using the actual size.

The system analyzes the ITT needs of VP tunnel subinterfaces and configures the parent physical interface accordingly. Enabling this command mode increases the use of processor and memory resources.

Examples   This example shows how to enable autominblock mode:

```
!
atm input-xlate-table autominblock
!
```

Related Commands

Command	Description
atm input-xlate-table minblock	Specifies the minimum ITT block size for a specific VPI on an interface.

atm input-xlate-table autoshrink

To shrink the existing Input Translation Table (ITT) blocks in-place when high numbered virtual circuits (VC's) are deleted, use the **atm input-xlate-table autoshrink** configuration mode command. To disable autoshrink, use the **no** form of this command.

> **atm input-xlate-table autoshrink**

> **no atm input-xlate-table autoshrink**

Syntax Description   This command has no arguments or keywords.

Defaults   Disabled.

Command Modes   Global configuration mode

Command History

Release	Modification
12.1(4)DB	This command was introduced on the Cisco 6400 NSP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   Be careful when enabling this command mode, because it increases the use of processor and memory resources.

> **Note**   This command cannot override the *blocksize* hints specified by using the **minblock**/**autominblock** commands.

Examples   This example shows how to shrink an ITT block in place and release the unrequired ITT resources when high numbered VCs are deleted from the configuration:

```
atm input-xlate-table autoshrink
!
interface atm 1/0/0
    no atm pvc 0 1010
    no atm pvc 0 1011
    exit
!
no atm input-xlate-table autoshrink
```

Related Commands	Command	Description
	atm input-xlate-table minblock	Specifies the minimum ITT block size for a specific virtual path identifier (VPI) on an interface.
	atm input-xlate-table autominblock	Enables automatic determination of minimum ITT block size needed for each VPI populated by PVC and Soft PVC source legs.

atm input-xlate-table minblock

To specify the minimum Input Translation Table (ITT) block size for a specific virtual path identifier (VPI) on an interface, use the **atm input-xlate-table minblock** interface configuration mode command. To remove the minimum block size specification, use the **no** form of this command.

> **atm input-xlate-table minblock vpi** *vpi- value blocksize* **force**

> **no atm input-xlate-table minblock vpi** *vpi-value*

Syntax Description

vpi-value	VPI to which the command applies. Values are in the range 0 to 255.
blocksize	Block size rounded up to the smallest power of 2 greater than or equal to the entered value. Values are in the range 32 to 16,384.
force	Indicates a user-entered value that is not overridden by autominblock analysis and is saved in configuration generation.

Defaults

No minimum block size is specified.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.1(4)DB	This command was introduced on the Cisco 6400 NSP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines

Ensure that the block size you specify corresponds to the desired virtual circuit (VC) usage, so that the system resource is not overused. ITT resource is used only when a connection is installed (when both interfaces that the VC transits are up).

This command is particularly useful when you anticipate the needs of switched virtual circuits (SVCs) transiting an interface and VPI, and you want to avoid the fragmentation associated with ITT growth. If the initial ITT block allocation fails and the actual block size needed [to accomodate a specific virtual channel identifier (VCI)] is less than the specified minimum block size, the software retries the allocation by using the actual size.

Note You cannot use this command on a virtual path (VP) tunnel subinterface. To specify minimum block size for a VP tunnel subinterface, configure this command on the main interface.

Examples   This example shows how to specify minimum block size for VPIs on an interface by manual
configuration:

```
!
interface atm 1/0/0
        atm input-xlate-table minblock vpi 0 1024 force
        atm input-xlate-table minblock vpi 1 2048 force
        atm input-xlate-table minblock vpi 4 1024 force
        exit
!
```

Related Commands

Command	Description
atm input-xlate-table autominblock	Automatically determines the minimum ITT block size needed for each VPI that is populated by PVCand Soft PVC source legs.

atm snoop interface atm

To set the current port snooping configuration and actual register values for the highest ATM interface, use the **atm snoop interface atm** interface configuration command.

atm snoop interface atm *monitored-port* [**direction** *dir*]

Syntax Description

monitored-port	Slot, subslot, and port number for the ATM interface to be monitored. The port can be any port except the NSP ATM 0/0/0 port or the test port.
dir	Specified as receive or transmit and determines the direction of the cell traffic to monitor.

Defaults

Receive

Command Modes

Interface configuration on the snoop test port.

Usage Guidelines

The **atm snoop interface atm** subcommand applies only if the previously specified port is the highest system port residing on card 8 and subcard 1 (which has been shut down). If these conditions are met, the subcommand enables the snoop test port. Cells transmitted from the snoop test port are copies of cells transmitted to or from the monitored port. Transmissions in only one direction are captured.

When a port is in snoop mode, any prior permanent virtual connections to the snoop test port remain in the down state.

The port number of the test port depends on the card type.

Examples

The following example shows how to configure the highest port in the snoop mode to monitor port card 1, subcard0, and port 1 in the transmit direction starting from the configuration mode:

```
Switch(config)# interface atm 8/1/1
Switch(config-if)# shutdown
Switch(config-if)# atm snoop interface atm 1/0/1 direction transmit
Switch(config-if)# no shutdown
```

Related Commands

show atm snoop

atm svc-upc-intent

To change the intended UPC mode to use on the cell flow received into the switch fabric for SVCs or destination legs of soft PVCs on an interface, use the **atm svc-upc-intent** command in interface configuration mode. Any change in this parameter is applied to SVCs or soft PVCs subsequently established on the interface. To assign the default value to the parameter, use the **no** form of this command.

atm svc-upc-intent [{**abr** | **cbr** | **vbr-rt** | **vbr-nrt** | **ubr**}] {**tag** | **pass** | **drop**}

no atm svc-upc-intent

Syntax Description	**abr** | **cbr** | **vbr-rt** | **vbr-nrt** | **ubr**	(Optional) Specifies the service category:
		• ABR—available bit rate
		• CBR—constant bit rate
		• VBR-RT—variable bit rate, real time
		• VBR-NRT—variable bit rate, non-real time
		• UBR—unspecified bit rate
	tag	Cells received on the interface violating the traffic contract have their CLP bit set prior to entering the switching fabric.
	pass	Cells received on the interface are passed to the switching fabric with no change, regardless of their conformance to the traffic contract.
	drop	Cells received on the interface violating the traffic contract are dropped.

Defaults   **Pass** for all service categories

Command Modes   Interface configuration

Command History

Release	Modification
11.1(4)	This command was introduced on the LS1010.
12.2(4)B	This command was modified for the Cisco 6400 NSP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines   This configuration parameter determines the UPC to use for SVCs and for the destination leg of soft VC and VP. If policing is desired, it should be applied once for traffic entering a network.

Examples   In the following example, the intended UPC for SVCs on an interface is set to tagging.

Switch(config-if)# **atm svc-upc-intent tag**

In the following example, the UBR traffic on an interface is passed while all other traffic is policed:

Switch(config-if)# **atm svc-upc-intent ubr pass**
Switch(config-if)# **atm svc-upc-intent cbr tag**
Switch(config-if)# **atm svc-upc-intent vbr-rt tag**
Switch(config-if)# **atm svc-upc-intent vbr-nrt tag**
Switch(config-if)# **atm svc-upc-intent abr drop**

Related Commands

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

auto-ferf

To allow an automatic far end receive failure (**FERF**) to be inserted when an incoming alarm is received, use the **auto-ferf** interface configuration command. To cancel automatic FERF insertion, use the no form of this command.

auto-ferf {**los** | **oof** | **red** | **ais** | **lcd** }

no auto-ferf { **los** | **oof** | **red** | **ais** | **lcd**}

Syntax Description

los	Loss of signal.
oof	Out of frame.
red	Indicates a major alarm. Does not apply to the DS3 NLC.
ais	Alarm indication signaling.
lcd	Loss of cell delineation.

Defaults   **auto-ferf los**
auto-ferf oof
auto-ferf red
auto-ferf ais
auto-ferf lcd (applies to **non-plcp** mode only)

Command Modes   Interface configuration

Command History

Release	Modification
12.0(1)DB	This command was introduced Cisco 6400 NSP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   This command applies to the DS3 interfaces only.

Cisco 6400 Command Reference   ■

auto-sync

To automatically synchronize the configuration between the Cisco 6400 primary and secondary redundant NSPs and NRPs, use the **auto-sync** redundancy subcommand. To disable automatic synchronization between redundant NSPs or NRPs, use the **no** form of this command.

auto-sync {**startup-config** | **bootvar** | **config-register** | **standard**}

no auto-sync {**startup-config** | **bootvar** | **config-register** | **standard**}

Syntax Description		
	startup-config	Specifies that the startup configuration be synchronized between the two redundant NSPs.
	bootvar	Specifies that the boot variables be synchronized between the two redundant NSPs. Boot variables are ROMMON environment variables used to control the booting process.
	config-register	Specifies that the configuration register be synchronized between the two redundant NSPs. The configuration register, stored in NVRAM, contains startup time parameters for the system.
	standard	Specifies that all objects be synchronized between the two redundant NSPs. In this case, all objects are the startup configuration, the bootvar, and the configuration register.

Defaults

No synchronization for individual objects. **Standard** is the default when auto-synchronization is enabled.

Command Modes

Main-cpu redundancy configuration

Usage Guidelines

To ensure that the configurations are identical between redundant NSPs or NRPs, you must use the **auto-sync** command. Otherwise, when operation changes from the primary to the secondary device, the operation of the switch or router might change if the configurations differ from one member of the redundant pair to the other.

Examples

The following example shows how to configure automatic synchronization of the startup configuration between redundant NSPs:

```
Switch# redundancy
Switch(config-r)# main-cpu
Switch(config-r-mc)# auto-sync startup-config
```

Related Commands

redundancy
main-cpu

clear facility-alarm

To clear the external alarm relays or the device memory for the requested alarm level or source reported on a Cisco 6400, use the **clear facility-alarm** EXEC command.

clear facility-alarm [**major** | **minor** | **critical**] [**source** {**sec-cpu** | **pem** {**0** | **1**} | **cardtype** {*slot* / *subslot*}}]

Syntax Description

major	Specifies that all major alarms be cleared.
minor	Specifies that all minor alarms be cleared.
critical	Specifies that all critical alarms be cleared.
source	Specifies the source of an alarm.
sec-cpu	Specifies the source of the alarm you want to clear as the secondary CPU. There is no other way to clear an alarm on this device.
pem	Specifies the source of the alarm you want to clear as one of the redundant power modules, either 0 or 1. There is no other way to clear an alarm on this device.
cardtype *slot/subslot*	Specifies the source of the alarm you want to clear as the device installed in the specified slot or subslot. There is no other way to clear an alarm on this device.

Defaults   If no operator is specified, all external alarms are cleared.

Command Modes   EXEC

Usage Guidelines   The **clear facility-alarm** command clears all of the specified external alarm indications. The alarm condition is still posted and can be seen by use of the **show facility-alarm status** command, and the LEDs are still illuminated. To clear the alarm status, you must remove the alarm condition at its source by specifying an alarm source with this command. When a source is specified, the memory of the specified device is cleared, thereby clearing the source of the alarm.

Examples   In the following example, only the minor alarms are cleared.

Switch> **clear facility-alarm minor**

Related Commands   **debug pmbox**
show facility-alarm status

clock source

To select a transmit clock source for a physical device such as a port, use the **clock source** interface configuration command. To return the clock source to the default, use the **no** form of this command.

clock source {**free-running** | **loop-timed** | **network-derived**}

no clock source {**free-running** | **loop-timed** | **network-derived**}

Syntax Description

free-running	The transmit clock is derived from the NSP.
loop-timed	The transmit clock is derived from the receive (rx) clock.
network-derived	The transmit clock is derived from the port system clock specified at highest priority when you use the **network-clock-select** global configuration command.

Defaults

loop-timed

Command Modes

Interface configuration

Command History

Release	Modification
12.0(1)DB	This command was introduced on the Cisco 6400 NSP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines

This command allows selection of the transmit clock source for a port's physical device. When a transmit clock port is set to **free-running**, the port uses the NSP oscillator for clocking.

Examples

The following example shows how to enable the loop-timed clocking mode.

Switch(config-if)# **clock source loop-timed**

Related Commands

framing (interface configuration)
network-clock-select

debug config-download

The Cisco 6400 uses a download protocol to download the NRP-2 startup configuration from the NSP. The download protocol and data pass through the NRP-2 PAM mailbox serial interface. To view the configuration download protocol message header types as they are received on the PAM mailbox serial interface, use the **debug config-download** EXEC command. The **no** form of this command disables debugging output.

> **debug config-download**
>
> **no debug config-download**

Syntax Description   This command has no keywords or arguments.

Defaults   Disabled

Command History

Release	Modification
12.1(4)DC	This command was introduced on the Cisco 6400 NSP to support the NRP-2.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples   In the following example, the **debug config-download** command is used to display configuration download protocol monitoring information:

```
Switch# debug config-download
CDNLD debugging is on
Switch#
00:01:39:CDNLD(6/0):WRR
00:01:39:CDNLD(6/0):DR
00:01:39: do_chksum num_bytes = 610
00:01:39: calc cksum = 0xC405
00:01:39:CDNLD(6/0):DR
```

Related Commands

Command (Entered on the NRP-2)	Description
NRP-2# **debug pmbox rx-path config-download**	Displays configuration download messages received by the NRP-2 PAM mailbox serial interface.
NRP-2# **debug pmbox tx-path config-download**	Displays configuration download messages transmitted by the NRP-2 PAM mailbox serial interface.

debug disk-mirror

To display debug messages for IFS call events, disk write events, and disk synchronization events, use the **debug disk-mirror** EXEC command. To disable debugging output, use the **no** form of this command.

debug disk-mirror

no debug disk-mirror

Syntax Description   This command has no keywords or arguments.

Defaults   Disabled

Command History

Release	Modification
12.1(5)DB	This command was introduced on the Cisco 6400 NSP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples   The following example shows how to enable debugging for disk mirroring. The example also shows the messages that appear when copying a file to the PCMCIA disks in disk slot 0 of both NSPs:

Switch# **debug disk-mirror**

NSP DISK MIRROR debugging is on
Switch# **copy running-config mir-disk0:**
...
21:38:06:DISK-MIRROR:enter mfs_open()...
21:38:06:DISK-MIRROR:leave mfs_open()
...
21:38:06:DISK-MIRROR:enter mfs_write()...
21:38:06:DISK-MIRROR:leave mfs_write()
...
21:38:06:DISK-MIRROR:enter mfs_close()...
21:38:06:DISK-MIRROR:leave mfs_close()

debug image-download

The Cisco 6400 uses a download protocol to download the NRP-2 image from the NSP or integrated file system (IFS). The download protocol and data pass through the NRP-2 PAM mailbox serial interface. To view the image download protocol message header types as they are received on the PAM mailbox serial interface, use the **debug image-download** EXEC command. The **no** form of this command disables debugging output.

debug image-download [**tftp**]

no debug image-download

Syntax Description		
	tftp	Also displays TFTP download messages.

Defaults   Disabled

Command History

Release	Modification
12.1(4)DB	This command was introduced on the Cisco 6400 NSP to support the NRP-2.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Related Commands

Command (Entered on the NRP-2)	Description
NRP-2# **debug pmbox rx-path image-download**	Displays image download messages received by the NRP-2 PAM mailbox serial interface.
NRP-2# **debug pmbox tx-path image-download**	Displays image download messages transmitted by the NRP-2 PAM mailbox serial interface.

facility-alarm

To enter explicit threshold temperatures for minor and major alarms, use the **facility-alarm** global configuration command. To disable the alarm for the minor or major temperature threshold, use the **no** form of this command.

> **facility-alarm** [**intake-temperature** | **core-temperature**] [**minor** {°*C*}] [**major** {°*C*}]

> **no facility-alarm** [**intake-temperature** | **core-temperature**] [**minor** {°*C*}] [**major** {°*C*}]

Syntax Description		
	intake-temperature	Specifies the minor and major temperature thresholds for the reading at the intake airflow.
	core-temperature	Specifies the minor and major temperature thresholds for the reading at the core of the chassis.
	minor	Specifies the temperature threshold for the minor alarm in degrees Celsius. If no value is specified, the threshold is reset to the default value.
	major	Specifies the temperature threshold for the major alarm in degrees Celsius. If no value is specified, the threshold is reset to the default value.

Defaults   Disabled

Command Modes   Global configuration

Usage Guidelines   The Cisco 6400 environmental monitoring hardware includes a digital thermometer that measures the intake airflow temperature at the hottest section of the chassis. The minor, major, and critical temperature defaults are empirically determined values that vary depending on the number and type of cards installed in the chassis. The **facility-alarm** command allows you to override the empirically determined default values. The **no** form of this command allows you to disable alarms for the selected alarm type.

Critical alarms cannot be disabled and the threshold cannot be changed. These alarms are defined as those that are triggered just before the system powers itself off.

Examples   In the following example, a setting is selected for the chassis core temperature at which a major alarm will be triggered.

Switch(config)# **facility-alarm core-temperature major 105**

Related Commands   **clear facility-alarm**
show facility-alarm status

framing

To select the frame type for the data line, use the **framing** controller interface configuration command.

framing { **m23adm** | **m23plcp** | **cbitadm** | **cbitplcp** }

Syntax Description

m23adm	The framing mode is M23 ADM.
m23plcp	The framing mode is M23 PLCP.
cbitadm	The framing mode is C-Bit ADM.
cbitplcp	The framing mode is C-Bit PLCP.

Defaults

DS3 default is **cbitplcp**.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(1)DB	This command was introduced on the Cisco 6400 NSP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines

In the DS3 environment, this subcommand allows selection of DS3 framing mode to M23 ADM, M23 PLCP, C-Bit ADM, or C-Bit PLCP.

Examples

The following example shows **m23adm** as the frame type:

Switch(config-if)# **framing m23adm**

Related Commands

show controllers

hw-module

hw-module (image)

To identify the image to download to a specific NRP-2 processor, use the **hw-module (image)** global configuration command. To remove an NRP-2 image specification, use the **no** form of this command.

> **hw-module slot** *slot* **image** *image* **priority** *priority*

> **no hw-module slot** *slot* **image** *image* **priority** *priority*

hw-module (config-register)

To change the configuration register settings for the NRP-2, use the **hw-module (config-register)** global configuration command.

> **hw-module slot** *slot* **config-register** *value*

hw-module (reset)

To simulate removal and insertion of a device installed in the Cisco 6400 chassis, use the **hw-module (reset)** EXEC command.

> **hw-module** {**slot** *slot* | **subslot** *slot*/*subslot* | **main-cpu** | **sec-cpu** | **nsp** {**A** | **B**}} **reset**

hw-module (shutdown)

To simulate removal or shutdown of a device installed in the Cisco 6400 chassis, use the **hw-module (shutdown)** global configuration command. The device remains in removed state even through system reloads. To return the device to inserted state in the chassis, use the **no** form of this command.

> **hw-module** {**slot** *slot* | **subslot** *slot*/*subslot* | **main-cpu** | **sec-cpu** | **nsp** {**A** | **B**}} **shutdown**

> **no hw-module** {**slot** *slot* | **subslot** *slot*/*subslot* | **main-cpu** | **sec-cpu** | **nsp** {**A** | **B**}} **shutdown**

Syntax Description

config-register	Specifies a change in the configuration register settings.
image	Specifies an image to assign to selected slot.
image	Any valid integrated file system (IFS), including: • *filename*—Specifies an image in the "images" directory of the NSP PCMCIA disk. • **disk0:***directory/path/filename*—Specifies an image on the NSP PCMCIA disk but not in the "images" directory. • **tftp:**...*/filename*—Specifies an image on a TFTP server.
main-cpu	Specifies that the main CPU should be reset. Allows you to reset the main CPU regardless of the CPU you are currently logged in to.
nsp {**A**	**B**}	Specifies the slot (0A or 0B) of the NSP to be reset.
priority	Specifies the priority of the selected image for the slot.
priority	Priority value. The priority range is from 1 (highest) to 4 (lowest).
reset	Simulates card removal and insertion of the specified device.
sec-cpu	Specifies that the secondary CPU should be reset. Allows you to reset the secondary CPU regardless of the CPU you are currently logged into.

shutdown	Simulates shutdown or removal of the designated card from the system. Holds card in shutdown or removed state, even through system reloads.
slot *slot/subslot*	Specifies the slot or subslot of the device. Slot range is 1-8, subslot range is 0-1.
value	Hexadecimal or decimal value that represents the 16-bit configuration register value that you want to use the next time the router is restarted. The value range is from 0x0000 to 0xFFFF (0 to 65,535 in decimal).

Specific bit values:

- 0x2101—Default configuration register setting. Combines the behaviors of the 0x2000, 0x0100, and 0x0001 bit values.

- 0x2000—If set (as it is by default), ROMMON runs from the image found in BootFROM1, if valid. If clear, ROMMON always runs the ROMMOM image in BootFROM0.

- 0x0100—Break or abort has no effect.

- 0x0001—NRP-2 boots the image specified with the **hw-module(image)** command.

- 0x0000—NRP-2 boots to ROMMON.

Defaults

hw-module (image)
No image identified

hw-module (config-register)
Configuration register value is 0x2101

hw-module (reset)
No default behavior or values

hw-module (shutdown)
Shutdown disabled

Command Modes

Global configuration

The **reset** version of this command can be used in EXEC mode.

Command History

Release	Modification
11.2 GS	This command was introduced.
11.3(6)AA	This command was implemented on the Cisco AS5800.
12.0(1)DB	This command was implemented on the Cisco 6400 NSP.
12.0(9)SL	This command was implemented on the Cisco 10000 Edge Services Router (ESR).
12.0(1a)W5(5b)	This command was implemented on the Catalyst 8540 Multiservice ATM Switch Router (MSR), Catalyst 8510 MSR, and LightStream 1010 ATM switch router.

Release	Modification
12.1(4)DB	The **image** and **config-register** versions of this command were introduced on the Cisco 6400 NSP to support the NRP-2.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines

hw-module (image)

Enter at least one instance of this command for each NRP-2 in the Cisco 6400 system. Without the command in the NSP configuration, the NRP-2 attempts to load the default image (c6400r2sp-g4p5-mz) from the NSP disk0:/images/ directory. If the image cannot be located, the NRP-2 is not able to boot.

Cisco recommends that you store all NRP-2 images on the NSP PCMCIA "disk0:/images" directory, but you can also store NRP-2 images on any integrated file system (IFS) device, including disk1 and TFTP, FTP, or rcp servers.

For images in the disk0:/images directory, you can use a shortened **no** version of the command to remove an NRP-2 image specification: **nohw-module** *filename*.

The **hw-module(image)** command performs the same function for the NRP-2 as the **boot system** global configuration command does for the NRP-1. Because NRP-2 boot information is stored on the NSP, the **hw-module(image)** command is entered on the NSP.

Note   The **boot system** global configuration command is not supported on the NRP-2.

hw-module (config-register)

This command enables you to change the NRP-2 configuration register settings.

The **hw-module (config-register)** command performs the same function for the NRP-2 as the **config register** global configuration and **confreg** ROMMON mode commands do for the NRP-1. Because the NRP-2 ROM state information is stored on the NSP, the **hw-module (config-register)** command is entered on the NSP.

Note   The **config register** global configuration and **confreg** ROMMON mode commands are not supported on the NRP-2.

hw-module (reset)

This is the only version of the **hw-module** command that can be entered in EXEC mode. It can be used to reload the specified device from the NSP.

hw-module (shutdown)

This command keeps the selected card offline, even through system reloads.

Examples

hw-module (image)

In the following example, the NRP-2 in slot 2 of the Cisco 6400 chassis has three images assigned with different priorities, while the NRP-2 in slot 3 has only one image assigned:

```
Switch(config)# hw-module slot 2 image c6400r2sp-g4p5-mz.DC priority 2
Switch(config)# hw-module slot 2 image tftp://10.1.1.1/c6400r2sp-g4p5-mz.DC priority 3
Switch(config)# hw-module slot 2 image disk0:MyDir/c6400r2sp-g4p5-mz.DC priority 4
Switch(config)# hw-module slot 3 image c6400r2sp-g4p5-mz.DC priority 2
```

Timesaver   If you don't use all the priority values for NRP-2 images, consider leaving priority 1 free for new or temporary images.

hw-module (config-register)

In the following example, the configuration register setting causes the NRP-2 in slot 4 to boot only to ROMMON mode:

```
Switch(config)# hw-module slot 4 config-register 0x0
```

In the following example, the configuration register setting causes the NRP-2 in slot 2 to boot the image specified with the **hw-module(image)** command:

```
Switch(config)# hw-module slot 2 config-register 0x1
```

hw-module (reset)

In the following example, the device in slot 5 is reset:

```
Switch# hw-module slot 5 reset
*Sep 28 22:30:56.590:%NSP_OIR-6-FULL_CREM:Card NRP2 removed from slot:5
*Sep 28 22:30:58.510:%NSP_OIR-6-FULL_CINS:Card NRP2 inserted into slot:5
*Sep 28 22:30:58.510:%NSP_OIR-6-FULL_ONLINE:Card NRP2, slot:5, being brought online
```

In the following example, the NSP in slot 0A is reset:

```
Switch# hw-module nsp A reset
```

hw-module (shutdown)

In the following example, the device in slot 4 is shutdown:

```
Switch(config)# hw-module slot 4 shutdown
```

interface

To configure an interface type and enter interface configuration mode, use the **interface** global configuration command.

> **interface** *type slot/subslot/port*

> **interface** *type number*

To configure a subinterface, use the interface global configuration command.

> **interface** *type slot/subslot/port.vpt#*

> **interface** *type slot/subslot/port.subinterface#* [**multipoint** | **point-to-point**]

Syntax Description

type	Type of interface to be configured. Refer to Table 3-2 for a list of keywords.
number	Integer used to identify the interface.
slot	Interface slot number. The numbers are assigned at the factory at the time of installation or when the card is added to a system. The number can be displayed with the **show interface** command. The slots are numbered from left to right.
subslot	Backplane subslot number. The value can be **0** or **1**.
port	Port number of the interface.
.vpt	Virtual path tunnel number for subinterface on physical ATM ports.
.subinterface	Subinterface number in the range 1 to 4,294,967,293. The number that precedes the period (.) must match the subinterface number.
multipoint	Specifies a multipoint subinterface. This option applies only to the interface ATM0/0/0.
point-to-point	Specifies a point-to-point subinterface. The default is **multipoint**. This option applies only to the interface ATM 0/0/0.

Command Modes   Global configuration

Usage Guidelines   For information or output for the **NRP interface atm** command, refer to the *Cisco IOS 12.0 Wide-Area Networking Command Reference*.

Table 3-2   Interface Type Keywords

Keyword	Interface Type
async	Auxiliary port line used as an asynchronous interface.
atm	ATM interface.
bvi	Bridge-group virtual interface.
cbr	CBR interface.
dialer	Dialer interface.

Table 3-2   Interface Type Keywords (continued)

Keyword	Interface Type
ethernet	Ethernet IEEE 802.3 interface.
group-async	Master asynchronous interface.
lex	Lex interface.
loopback	Software-only loopback interface that emulates an interface that is always running. It is a virtual interface supported on all platforms. The *interface number* is the number of the loopback interface you want to create or configure. There is no limit on the number of loopback interfaces you can create.
null	Null interface.
tunnel	Tunnel interface, used to declare a TSP tunnel interface. The tunnel interface number is in the range 0 to 65535.
virtual-template	Virtual template interface.
virtual-tokenring	Virtual Token Ring interface.
vlan	Catalyst 5000 VLAN interface.

Examples   The following example shows the start of the ATM interface on slot 1, subslot 0, and port 1 configuration using the **interface** global configuration command:

```
Switch(config)# interface atm 1/0/1
Switch(config-if)#
```

In the following example, a VP tunnel is created with VPI 50 on slot 1, subslot 0, and port 1. The subinterface configuration mode is entered for the VP tunnel, by using the **interface** global configuration command:

```
Switch(config)# interface atm 1/0/1
Switch(config-if)# atm pvp 50
Switch(config-if)# interface atm 1/0/1.50
Switch(config-subif)#
```

In the following example, configuration begins on the NRP interface ATM 0/0/0, by using the **interface** global configuration command:

```
Router(config)# interface atm 0/0/0
Router(config-if)#
```

In the following example, the **interface** global configuration command is used to create a point-to-point subinterface on the NRP ATM 0/0/0 interface and enter the subinterface configuration mode:

```
Router(config)# interface atm 0/0/0.1 point-to-point
Router(config-subif)#
```

In the following example, configuration of the BVI 1 interface on the NSP begins by using the **interface** global configuration command:

```
Switch(config)# interface bvi 1
Switch(config-if)#
```

Related Commands   **show interface**

ip address

To set a primary or secondary IP address for an interface or to use DHCP to set the interface address, use the **ip address** interface configuration command. To remove an IP address or disable IP processing, use the **no** form of this command.

ip address [*ip-address mask* [**secondary**] | **negotiated**]

no ip address [*ip-address mask* [**secondary**] | **negotiated**]

Syntax Description	
ip-address	IP address.
mask	Mask for the associated IP subnet.
secondary	Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.
negotiated	Specifies the use of DHCP to obtain the IP address, subnet mask, and default route.

Defaults   Negotiated.

Command Modes   Interface configuration

Usage Guidelines   The **negotiated** (default) option for this command allows the system to act as a DHCP client and automatically set the IP address, subnet mask, and default route for the specified interface. On the NSP, this command applies only to the Ethernet 0/0/0 and ATM 0/0/0 interfaces.

You can disable IP processing on a particular interface by removing its IP address with the **no ipaddress** command. If the switch detects another host using one of its IP addresses, it prints an error message on the console.

The optional keyword **secondary** allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates using the secondary source addresses. IP broadcasts and ARP requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There might not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need to have 300 host addresses. Using secondary IP addresses on the switches, you can have two logical subnets using one physical subnet.

- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network by means of secondary addresses.

Note   If any switch on a network segment uses a secondary address, all other switches on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.

Examples   In the following example, 172.31.1.27 is the primary address and 192.168.7.17 and 192.168.8.17 are secondary addresses for Ethernet interface 0/0/0:

Switch(config)# **interface ethernet 0/0/0**
Switch(config-if)# **ip address 172.31.1.27 255.255.255.0**
Switch(config-if)# **ip address 192.168.7.17 255.255.255.0 secondary**
Switch(config-if)# **ip address 192.168.8.17 255.255.255.0 secondary**

Related Commands   **show interface**

lbo

To set the line buildout to various lengths, use the **lbo** interface configuration command. For the DS3 NLC, the syntax is:

lbo {**short** | **long**}

Syntax Description

short	Sets the line buildout up to 255 feet.
long	Sets the line buildout to more than 255 feet.

Defaults

The default is **short.**

Command Modes

Interface configuration

Command History

Release	Modification
12.0(1)DB	This command was introduced on the Cisco 6400 NSP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines

The **lbo** command applies on DS3 interfaces only.

Examples

The following example illustrates how to set the line buildout to more than 255 feet for a DS3 NLC:

Switch(config-if)# **lbo long**

main-cpu

To switch to the **main-cpu** submode of the redundancy mode, use the **main-cpu** redundancy command.

    main-cpu

Syntax Description   This command has no arguments or keywords.

Command Modes   Redundancy

Usage Guidelines   After you enter the main-cpu submode, you can use the **auto-sync** command to synchronize the configuration between the primary and secondary route processors based on the primary configuration. In addition, you can use all of the redundancy commands that are applicable to the main CPU.

Examples   The following example shows how to switch to the main-cpu submode of redundancy mode.

Switch(config)# **redundancy**
Switch(config-r)# **main-cpu**
Switch(config-r-mc)#

Related Commands   **aps mode**
auto-sync
redundancy
show redundancy

mirror

To enable PCMCIA disk mirroring or specify mirroring characteristics, use the **mirror** main-cpu configuration command. To disable PCMCIA disk mirroring, use the **no** form of this command.

mirror [**all** | **threshold** *size*]

no mirror

Syntax Description

all	(Optional) Specifies that all files will be mirrored blindly (without comparing file names, sizes, and time stamps).
threshold	(Optional) Specifies to blindly copy files smaller than the file size threshold.
size	(Optional) Threshold size in megabytes (MB).

Defaults   Enabled with file threshold size of 0 MB

Command Modes   Main-cpu configuration

Command History

Release	Modification
12.1(5)DB	This command was introduced on the Cisco 6400 NSP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   When you enter the **no mirror** command, any mirroring characteristics that were previously specified with the **all** and **threshold** keywords are permanently removed.

If disk synchronization is in progress when you enter the **no mirror** command, a prompt warns you that disk synchronization will terminate. You can either proceed with or cancel your disable request.

Press **Return** to proceed with disabling disk mirroring and terminating the unfinished disk synchronization:

Switch(config-r-mc)# **no mirror**

→ Disk synch will terminate. Proceed with disable? [confirm] **<Cr>**
Switch(config-r-mc)#
21:35:19:%DISKMIRROR-6-FINISH:Disk Sync Finished (0 files syncd; 6 failed)
Switch(config-r-mc)#

Type **no** to cancel the **no mirror** command and to allow disk synchronization to continue:

Switch(config-r-mc)# **no mirror**

→ Disk synch will terminate. Proceed with disable? [confirm] **no**
Switch(config-r-mc)#

Examples   In the following example, PCMCIA disk mirroring is disabled:

```
!
redundancy
 main-cpu
  auto-sync standard
  no mirror
  !
```

In the following example, PCMCIA disk mirroring is enabled and set to copy all files blindly:

```
!
redundancy
 main-cpu
  auto-sync standard

  mirror all
  !
```

In the following example, PCMCIA disk mirroring is enabled with a specified files size threshold of 2MB:

```
!
redundancy
 main-cpu
  auto-sync standard

  mirror threshold 2
  !
```

Related Commands

Command	Description
redundancy sync	Copies the data from one PCMCIA disk to its mirror disk.
show redundancy sync-status	Displays status of disk mirroring and disk synchronization.

network-clock-select

Use the **network-clock-select** global configuration command to specify selection priority for the clock sources. Use the **no** form of this command to cancel the network clock selection.

> **network-clock-select** {*priority* {**ATM** *slot*/*subslot*/*port* | **BITS** | **system**} | **BITS** {**E1** | **T1**} | **revertive**}

> **no network-clock-select** {*priority* {**ATM** *slot*/*subslot*/*port* | **BITS** | **system**} | **BITS** {**E1** | **T1**} | **revertive**}

Syntax Description

priority	Specifies the priority, between 1 (highest) and 4.
ATM	ATM interface on NSP.
slot/*subslot*/*port*	Specifies the slot, subslot, and port number of the ATM interface.
BITS	Selects the BITS input as the network clock source.
system	The free running local clock oscillator on the NSP-S3B.
E1	Configures the BITS port as E1.
T1	Configures the BITS port as T1.
revertive	Automatic switchover to highest priority clock source when available.

Defaults   System clock is the priority 5 clock source.

Command Modes   Global configuration

Command History

Release	Modification
11.1 CA	This command was introduced for ATM-CES interfaces.
11.2	This command was introduced for the LightStream 1010.
12.0	This command was modified for the Catalyst 8510 MSR, Catalyst 8540 MSR, and LightStream 1010.
12.0(7) DB	This command modified for the Cisco 6400 NSP-S3B .
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines   You can specify up to four clock priorities. If the **network-clock-select revertive** command is used, the highest priority active interface in the router supplies the primary reference source to all other interfaces that require network clock synchronization services.

The fifth priority is always the system, or local clock oscillator on the NSP. You cannot configure the priority 5 clock source.

Examples   The following example shows how to configure the network clock as revertive and assign clock sources to each available priority:

```
Switch(config)# network-clock-select revertive
Switch(config)# network-clock-select bits e1
Switch(config)# network-clock-select 1 bits
Switch(config)# network-clock-select 2 ATM1/0/0
Switch(config)# network-clock-select 3 ATM5/0/0
Switch(config)# network-clock-select 4 ATM7/0/0
```

Related Commands

Command	Description
show network-clocks	Displays network clock status.

nrps

To telnet from the NSP to the NRP-2, use the **nrps** EXEC command alias.

nrps *slot*

Syntax Description

slot	Slot number of the NRP-2 to which you want to telnet. Valid values are 1 to 8.

Defaults   No default behavior or values.

Command Modes   EXEC (alias)

Command History Not applicable for command aliases

Usage Guidelines This is a command alias that telnets to the NRP-2.

You need to set the VTY line password before you can telnet to the NRP-2.

Examples In the following example, the user telnets from the NSP to the NRP-2 in slot 4 of the Cisco 6400 chassis, enters privileged EXEC mode, and then exits the Telnet session.

```
NSP# nrps4
Trying 10.4.0.2 ... Open

Router> enable
Router# exit

[Connection to 10.4.0.2 closed by foreign host]
NSP#
```

redundancy

To configure two full-height slots, two half-height slots, or the main CPU for redundant operation, use the **redundancy** global configuration command. The **redundancy** command starts a configuration submode, where the redundant configuration is specified.

redundancy

Syntax Description   None

Defaults   Disabled

Command Modes   Global configuration

Usage Guidelines   The **redundancy** command starts a configuration submode for setting slot and subslot redundancy. The exact redundancy implementation between a pair of redundant entities is a property of the objects actually installed in the chassis.

Only adjacent (odd and even) slot pairs can be configured for redundancy. When a slot is configured for redundancy, both the subslots, if there are any, are automatically configured for redundancy. When subslots are configured for redundancy, all ports on the two subslots are redundant.

Examples   The following example shows how to configure the two Cisco 6400 NRPs installed in slots 1 and 2 for redundant operation:

Switch(config)# **redundancy**
Switch(config-r)# **associate slot 1**

Related Commands   **aps mode**
main-cpu
redundancy force-failover
show redundancy

redundancy force-failover

To force the current primary and secondary devices in a redundant pair to change roles, use the
redundancy force-failover EXEC command.

redundancy force-failover {*slot* | *slot/subslot* | *slot/subslot* | **main-cpu**}

Syntax Description		
slot *slot/subslot*	Specifies the slot or subslot for one member of a redundant pair, where the primary/secondary relationship between the two entities is reversed.	
main-cpu	Specifies that the primary/secondary relationship between the two available NSPs be reversed.	

Defaults   Disabled

Command Modes   EXEC

Usage Guidelines   The **redundancy force-failover** command can be used to force a change in the primary/secondary
relationship required for software and hardware upgrade situations. This command has no effect on
interfaces that are running in SONET linear 1+1 nonreverting unidirectional APS mode. To reverse the
roles of two redundant ports, use the **aps force** command.

This command does not generate an alarm (as a hardware reset would).

Examples   In the following example, the primary/secondary relationship is reversed between the router card in
slot 2 and its redundant partner. The other slot in the redundant pair is not specified in this command.
You can use the **show redundancy** command to view the configured redundant pairs.

Switch# **redundancy force-failover slot 2**

Related Commands   redundancy
show redundancy

redundancy sync

To initiate disk synchronization, or copy the data from one PCMCIA disk to another, use the **redundancy sync** EXEC command.

redundancy sync [**disk0** | **disk1** | **local**] [**reverse**] [**all**]

Syntax Description

disk0	Specifies the PCMCIA disks in slot 0 of the redundant NSPs.
disk1	Specifies the PCMCIA disks in slot 1 of the redundant NSPs.
local	Copies data from disk0: to disk1: in the primary NSP.
reverse	Specifies reverse synchronization (copies data from the secondary NSP to the primary NSP).
all	Specifies to copy all files blindly (without comparing file names, sizes, and time stamps).

Defaults

With no keywords entered, this command copies data from disk0: of the primary NSP to disk0: of the secondary NSP. The system compares files between the PCMCIA disks and does not copy files with matching file names, sizes, and time stamps.

Command Modes

EXEC

Command History

Release	Modification
12.1(5)DB	This command was introduced on the Cisco 6400 NSP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines

By default, when performing disk synchronization (either through disk mirroring or user initiation), the system compares files between the PCMCIA disks. The system does not copy files with matching file names, sizes, and time stamps. The **all** keyword specifies to copy all files without comparison.

Without the **all** keyword, and if the **mirror** main-cpu configuration command is configured with a file threshold size, only files smaller than the threshold will be copied without comparison.

Examples

The following example shows PCMCIA disk synchronization:

Switch# **redundancy sync disk0**

00:29:52:%DISKMIRROR-6-PROGRS:Disk Sync in Progress (disk0 to sec-disk0, 0%)
Switch#

The following example shows reverse disk synchronization:

Switch# **redundancy sync disk0 reverse**

Cisco 6400 Command Reference ■

redundancy sync

00:32:13:%DISKMIRROR-6-PROGRS:Disk Sync in Progress (sec-disk0 to disk0, 0%)
Switch#

The following example shows local disk synchronization:

Switch# **redundancy sync local**

00:32:13:%DISKMIRROR-6-PROGRS:Disk Sync in Progress (disk0 to disk1, 0%)
Switch#

Related Commands

Command	Description
mirror	Enables PCMCIA disk mirroring.
show redundancy sync-status	Displays status of disk mirroring and disk synchronization.

snmp-server forwarder

To enable the SNMPv3 proxy forwarder, use the **snmp-server forwarder** global configuration command. To disable the proxy forwarder, use the **no** form of this command.

snmp-server forwarder

no snmp-server forwarder

Syntax Description   This command has no arguments or keywords.

Defaults   Disabled

Command Modes   Global configuration

Command History

Release	Modification
12.1(4)DB	This command was introduced on the Cisco 6400 NSP to support the NRP-2.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   The SNMPv3 Proxy Forwarder feature enables all NSP and NRP-2 components of the Cisco 6400 system to be managed as one functional entity. With the Proxy Forwarder feature enabled, the NSP:

- Forwards all SNMPv3 formatted messages (such as manager requests to get or set data) destined for the NRP-2s
- Routes the SNMPv3 formatted traps from NRP-2s to the NSP combined Network Management Ethernet (NME) interface

When the NSP and NRP-2 are properly configured for SNMPv3 and the Proxy Forwarder feature, both the NSP and NRP-2 automatically generate a series of SNMP commands. Do not modify or delete the automatically generated commands; doing so might prevent SNMP from working properly.

Examples   In the following example, the NSP is configured to act as the proxy forwarder:

```
snmp-server group usmgrp v3 noauth
snmp-server user usmusr usmgrp v3
→  snmp-server forwarder
snmp-server host 10.100.100.100 vrf 6400-private version 3 noauth trapusr
```

The previous commands cause the NSP to automatically generate the following commands:

```
snmp-server engineID remote 10.3.0.2 vrf 6400-private 80000009030000107BA9C7A0
snmp-server user trapusr trapusr v3
snmp-server user trapusr trapusr remote 10.3.0.2 vrf 6400-private v3
snmp-server user usmusr usmgrp remote 10.3.0.2 vrf 6400-private v3
snmp-server group trapusr v3 noauth notify *tv.FFFFFFFF.FFFFFFFF
```

■ **snmp-server forwarder**

In the following example, the NRP-2 is configured to allow the NSP to act as the proxy forwarder:

```
snmp-server group usmgrp v3 noauth
snmp-server user usmusr usmgrp v3
snmp-server enable traps
snmp-server host 10.3.0.1 vrf 6400-private version 3 noauth trapusr
```

The previous commands cause the NRP-2 to automatically generate the following commands:

```
snmp-server user trapusr trapusr v3
snmp-server group trapusr v3 noauth notify *tv.FFFFFFFF.FFFFFFFF
snmp-server enable traps snmp authentication linkdown linkup coldstart
snmp-server enable traps config
snmp-server enable traps syslog
snmp-server enable traps bgp
snmp-server enable traps ipmulticast
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps rtr
```

Related Commands

The SNMPv3 Proxy Forwarder feature requires the NSP and NRP-2 to be configured by using specific options in the **snmp-server** global configuration commands:

NSP Command	Description
snmp-server group *groupname* **v3 noauth**	Configures a new SNMPv3 group.
snmp-server user *username groupname* **v3**	Configures a new user to the SNMPv3 group.
snmp-server host *host-address* **vrf 6400-private version 3 noauth** *username*	Specifies the recipient of NRP-2 SNMPv3 trap messages.

NRP-2 Command	Description
snmp-server group *groupname* **v3 noauth**	Configures a new SNMPv3 group. Make sure that the *groupname* matches that entered on the NSP.
snmp-server user *username groupname* **v3**	Configures a new user to an SNMPv3 group. Make sure that the *username* and *groupname* match those entered on the NSP.
snmp-server enable traps [**config** | **syslog** | **bgp** | **ipmulticast** | **rsvp** | **frame-relay** | **rtr** | **snmp authentication linkdown linkup coldstart**]	Enables the NRP-2 to send traps. Optionally, you can select from specific types of traps.
snmp-server host 10.*nrp2-slot***.0.1 vrf 6400-private version 3 noauth** *username*	Specifies the NSP as the recipient of SNMPv3 trap messages. The **10.***nrp2-slot***.0.1** IP address is the private address for the internal NSP interface to the NRP-2 PAM mailbox serial interface.

tag-switching advertise-local-tags

To control which tags are advertised and to which nodes they are advertised, use the **tag-switching advertise-local-tags** global configuration command. To disable advertisement of tags, use the **no** form of this command.

tag-switching advertise-local-tags [**for** *access-list-num* [**to** *access-list-num*]]

no tag-switching advertise-local-tags [**for** *access-list-num* [**to** *access-list-num*]]

Syntax Description

for *access-list-num*	Specifies an access list of prefixes that should be advertised.
to *access-list-num*	Specifies an IP access list of TDP peer prefixes that should receive advertisements.

Defaults

For all tags and to all peers

Command Modes

Global configuration

Usage Guidelines

Multiple **tag-switching advertise-local-tags** commands can be used. When multiple commands are entered, their effect is combined to determine an overall specification of how locally allocated tags are advertised.

Examples

In the following example, the router is configured to advertise all locally assigned tags to all TDP neighbors. The assumption is that before the command is entered, the default of no tag advertisement is in effect:

Switch(config)# **tag-switching advertise-local-tags**

In the following example, the router is configured to advertise tags for networks 10.101.0.0 and 10.221.0.0 to all TDP neighbors. The assumption is that before the commands are entered, the default of no tag advertisement is in effect:

Switch(config)# **access-list 1 permit 10.101.0.0 0.0.255.255**
Switch(config)# **access-list 4 permit 10.221.0.0 0.0.255.255**
Switch(config)# **tag-switching advertise-local-tags for 1**
Switch(config)# **tag-switching advertise-local-tags for 4**

In the following example, the router is configured to advertise all tags to all TDP neighbors except neighbor 10.101.0.8. The assumption is that before the commands are entered, the default of no tag advertisement is in effect:

Switch(config)# **access-list 1 permit any**
Switch(config)# **access-list 2 deny 10.101.0.8**
Switch(config)# **tag-switching advertise-local-tags**
Switch(config)# **tag-switching advertise-local-tags for 1 to 2**

4

Show Commands for the Cisco 6400 NSP

This chapter describes the show commands specific to the Cisco 6400 node switch processor (NSP). Additional commands used to configure and monitor the Cisco 6400 NSP are described in:

- Chapter3, "Commands for the Cisco 6400 NSP"

- *Cisco ATM and Layer 3 Switch Router Command Reference*, available at www.cisco.com or on the Documentation CD-ROM.

show aps

To display the SONET APS configuration for each redundant interface, use the **show aps** command.

show aps

Command Modes   EXEC

Usage Guidelines   This command displays the APS status of all cards configured for APS mode linear 1+1 nonreverting unidirectional operation. The output is closely associated with the generation of K_1/K_2 bytes transmitted from the redundant interface.

Examples   The following is sample output from the **show aps** EXEC command.

```
Switch# show aps
ATM7/0/0: APS Lin NR Uni, Failure channel: Protection
       Active Channel: CHANNEL7/0/0, Channel stat: Good
       Port stat (w,p): (Good, Good)
ATM7/0/1: APS Lin NR Uni, Failure channel: Protection
       Active Channel: CHANNEL7/0/1, Channel stat: Good
       Port stat (w,p): (Good, Good)
```

Table 4-1 describes the fields shown in the display.

Table 4-1   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 nonreverting mode. (Default configuration.)
Uni	This interface is operating in unidirectional mode. (Default configuration.)
Failure channel:	The name of the failure channel specified by the b_5-b_8 field of the K_1 byte used in APS operation. Options can be Protection or Working.
Active channel:	The number of the active channel specified as the physical channel in use. These values correspond to the physical slot/subslot/port used within the chassis.
Channel stat:	The status of the active channel specified by the b_1-b_4 field of the K_1 byte used in APS operation.
Port stat:	The status of the individual physical working (w) and protection (p) channels.

show atm input-xlate-table

To view the Input Translation Table utilization details, use the **show atm input-xlate table command in EXEC** mode.

> **show atm input-xlate table [inuse]**

Syntax Description

inuse	Shows a detailed list of in-use blocks by port and virtual path identifier (VPI) .

Defaults   No default behavior or values.

Command Modes   EXEC

Command History

Release	Modification
12.1(4)DB	This command was introduced on the Cisco 6400 NSP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Examples   The following example shows how to use the command to view the ITT utilization details—with and without the **inuse** keyword:

```
Switch> show atm input-xlate-table
Input Translation Table Free Blocks:
Block-start  Size    Bank
1        1       0
2        2       0
4        4       0
8        8       0
16       16      0
32       32      0
64       64      0
17408    64      0
128      128     0
17536    128     0
256      256     0
17664    256     0
512      512     0
17920    512     0
1024     1024    0
2048     2048    0
18432    2048    0
4096     4096    0
20480    4096    0
8192     8192    0
24576    8192    0
32769    1       1
32770    2       1
32772    4       1
```

```
32776     8     1
32784     16    1
32800     32    1
49248     32    1
32832     64    1
49152     64    1
49344     64    1
32896     128   1
33024     256   1
49408     256   1
33280     512   1
49664     512   1
33792     1024  1
50176     1024  1
34816     2048  1
51200     2048  1
36864     4096  1
53248     4096  1
40960     8192  1
57344     8192  1

Input Translation Table Total Free = 64350

Input Translation Table In Use (display combines contiguous blocks):
 Inuse-start  Inuse-end  Size
0        0          1
16384    17407      1024
17472    17535      64
32768    32768      1
49216    49247      32
49280    49343      64
```

The output of the command with the **inuse** keyword is:

```
Switch> show atm input-xlate-table inuse
Interface    VPI VP/VC Address Size
ATM0/1/0     0   VC  17472 64
ATM0/1/0     2   VP  32768 1
ATM0/1/2     0   VC  49216 32
ATM0/1/2     2   VP  0     1
ATM1/0/0     0   VC  49280 64
ATM1/0/0     9   VC  16384 1024
```

Related Commands	Command	Description
	atm input-xlate-table autominblock	Automatically determines the minimum ITT block size needed for each VPI populated by permanent virtual circuits (PVC's) and Soft PVC source legs.
	atm input-xlate-table autoshrink	Shrinks the existing ITT blocks in place when high-numbered virtual circuits (VC's) are deleted.

show controllers async

To display information on the NRP-2 PAM mailbox serial interface from the NSP, use the **show controllers async** EXEC command.

show controllers async

Syntax Description	This command has no arguments or keywords.
Defaults	No default behavior or values.
Command Modes	EXEC

Command History

Release	Modification
11.2	This command was introduced on the Cisco 1005 router.
11.3(2)T	This command was implemented on Cisco 3600 series routers.
12.1(4)DB	This command was implemented on the Cisco 6400 NSP to support the NRP-2.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines   On the Cisco 6400, the **show controllers async** command can be used on the NSP or NRP-2 to view information for the NRP-2 PAM mailbox serial interface.

Examples   In the following example, the **show controllers async** command is used to view the NRP-2 PAM mailbox serial interface from the NSP:

```
NSP# show controllers async
Async NRP2 Pam bus controller
TTY line 1 not available
TTY line 2 not available
TTY line 3 not available
TTY line 4 not available
TTY line 5 not available
TTY line 6
PAM bus data for mailbox at 0xA8A8FFC0
  magic1 = 0xDEADBABE, magic2 = 0x21524541
  in_data = 0x0000000D, out_data = 0x0000003E
  in_status.received_break = 0
  out_status.received_break = 0
  tx_owned = TRUE, rx_owned = FALSE
Buffer information
  Rx ttycnt 0
  Tx ttycnt 0
  Rx Buffs:inpk 0/0 inheadpk 0 dataq 0 0 0
       pakq 0 0 0
  Tx Buffs:outpk 0  txpkq 0 0 0
  Rx totalin 1302 Tx totalout 69
```

```
                        TTY line 7 not available
                        TTY line 8 not available
                        TTY line 9 not available
                        TTY line 10 not available
                        TTY line 11 not available
                        TTY line 12 not available
                        TTY line 13 not available
                        TTY line 14
                        PAM bus data for mailbox at 0xA8E8FFC0
                          magic1 = 0xDEADBABE, magic2 = 0x21524541
                          in_data = 0x00000000, out_data = 0x00000000
                          in_status.received_break = 0
                          out_status.received_break = 0
                          tx_owned = TRUE, rx_owned = FALSE
                        Buffer information
                          Rx ttycnt 0
                          Tx ttycnt 0
                          Rx Buffs:inpk 0/0 inheadpk 0 dataq 0 0 0
                                 pakq 0 0 0
                          Tx Buffs:outpk 0  txpkq 0 0 0
                          Rx totalin 0 Tx totalout 0
                        TTY line 15 not available
                        TTY line 16 not available
                        NSP#
```

show facility-alarm status

To show the current major and minor alarms and the thresholds for all user-configurable alarms on a Cisco 6400, use the **show alarm status** command.

show facility-alarm status

Syntax Description

This command has no keywords or arguments.

Command Modes

Global configuration

Usage Guidelines

The **show facility-alarm status** command displays all of the current major and minor alarms and the user-configurable alarm thresholds for temperature. The Cisco 6400 has physical connections to a highly visible alarm display within the Central Office. After an alarm condition is indicated (by LEDs or bells), the **show facility-alarm status** command can be used to determine the cause of the alarm.

Examples

The following is an example of the output from the **show facility-alarm status** command:

```
Switch# show facility-alarm status
Thresholds:
Intake minor 40 major 50 Core minor 55 major 53
SOURCE:Network Clock TYPE:Network clock source, priority level 2 down
SEVERITY:Minor ACO:Normal
SOURCE:NSP EHSA TYPE:Secondary failure SEVERITY:Minor ACO:Normal
SOURCE:ATM2/0/1 TYPE:Sonet major line failure SEVERITY:Major ACO:Normal
SOURCE:ATM6/0/1 TYPE:Sonet major line failure SEVERITY:Major ACO:Normal
SOURCE:ATM7/0/1 TYPE:Sonet major line failure SEVERITY:Major ACO:Normal
SOURCE:ATM6/1/0 TYPE:Sonet major line failure SEVERITY:Major ACO:Normal
SOURCE:ATM6/1/1 TYPE:Sonet major line failure SEVERITY:Major ACO:Normal
SOURCE:ATM7/1/1 TYPE:Sonet major line failure SEVERITY:Major ACO:Normal
```

Related Commands

debug pmbox

show redundancy

To show which slots, subslots, ports, and CPUs are defined as being redundant on the Cisco 6400, use the **show redundancy** command.

show redundancy [*slot/subslot*]

Syntax Description   This command has no keywords or arguments.

Command Modes   EXEC

Usage Guidelines   This command displays a redundancy configuration table showing each object in a redundant pair and indicating which object is currently the master. Chassis redundancy is displayed if no slot or subslot is specified. If a slot or subslot is specified, the redundancy configuration for only that slot is displayed.

Examples   The following is sample output from the **show redundancy** command on the NSP:

```
Switch# show redundancy
Preferred main-cpu : B
NSP A           : Primary
NSP B           : Secondary
```

The following is sample output from the **show redundancy** command on the NRP:

```
Router# show redundancy
Primary   NRP in slot 2, system configured non redundant

User EHSA configuration (by CLI config):
slave-console = off
keepalive    = on
config-sync modes:
  standard   = on
  start-up   = on
  boot-var   = on
  config-reg = on

NSP EHSA configuration (via pam-mbox):
redundancy       = off
preferred (slot 2) = yes

Debug EHSA Information:
NRP specific information:
Backplane resets      = 0
NSP mastership changes = 0

print_pambox_config_buff: pmb_configG values:
valid         = 1
magic         = 0xEBDDBE1 (expected 0xEBDDBE1)
nmacaddrs     = 1
run_redundant   = 0x0
preferred_master = 0x1
macaddr[0][0]   = 0010.7b79.af93
macaddr[1][0]   = 0000.0000.0000
```

```
EHSA pins:
peer present = 0
peer state   = SANTA_EHSA_SECONDARY
crash status: this-nrp=NO_CRASH(1) peer-nrp=NO_CRASH(1)

EHSA related MAC addresses:
peer bpe mac-addr = 0010.7b79.af97
my   bpe mac-addr = 0010.7b79.af93
```

Related Commands   **show nrp**

show redundancy sync-status

To display the status of PCMCIA disk mirroring and synchronization type, use the **showredundancysync-status** EXEC command.

show redundancy sync-status

Syntax Description   This command has no keywords or arguments.

Defaults   No default behavior or values.

Command Modes   EXEC

Command History

Release	Modification
12.1(5)DB	This command was introduced on the Cisco 6400 NSP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines   The command output displays several lines:

Line Number (from top)	Description of Output
1	Displays disk mirroring status (enabled or disabled). Also displays whether disk mirroring is configured to copy all files blindly (full sync), or compares file names, sizes, and time stamps before synchronizing data (proper sync).
2	Displays the file threshold size (0 MB is the default) configured with the **mirror** command.
3	Displays whether or not the secondary NSP is in the chassis.
4	Displays whether or not a PCMCIA disk is missing from disk slot 1 of the primary or secondary NSP.
5	Displays whether or not the disks in slot 0 are synchronized between the primary and secondary NSP.
6	Displays whether or not the disks in slot 1 are synchronized between the primary and secondary NSP.
7	Only appears while synchronization is in progress. Identifies which disks are being synchronized, and what percentage of the synchronization is complete.

Examples   The following example shows that disk mirroring is enabled and that disk synchronization is in progress:

→ Switch# **show redundancy sync-status**
Disk Mirror is enabled in configuration:proper sync
(Mirror threshold is 0 MB:smaller files will be copied blindly)

Peer Secondary NSP is present
disk1 or sec-disk1 is wrong or missing

mir-disk0 (disk0 -> sec-disk0):out of sync.
mir-disk1 (disk1 -> sec-disk1):out of sync.

→ Disk Mirror full sync is in progress (disk0 to sec-disk0, 23%)

Switch#

The following example shows that disk mirroring is enabled and that the PCMCIA disks in slot 0 of the NSPs are synchronized:

Switch# **show redundancy sync-status**
Disk Mirror is enabled in configuration:proper sync
(Mirror threshold is 0 MB:smaller files will be copied blindly)

Peer Secondary NSP is present
disk1 or sec-disk1 is wrong or missing

→ mir-disk0 (disk0 -> sec-disk0):in sync.
mir-disk1 (disk1 -> sec-disk1):out of sync.

Switch#

Related Commands

Command	Description
mirror	Enables PCMCIA disk mirroring.
redundancy sync	Copies the data from one PCMCIA disk to its mirror disk.

show tag-switching atm-tdp bindings

To display the requested entries from the ATM LDP label bindings database, use the following s**how tag-switching atm-tdp bindings** EXEC command.

> **show tag-switching atm-tdp bindings** [*A.B.C.D* {*mask* | *length*}]
> [**local-tag** | **remote-tag** *vpi vci*] [**neighbor atm** *slot/subslot/port*]
> [**remote-tag** *vpi vci*]

Syntax Description

A.B.C.D	Destination of prefix.
mask	Destination netmask prefix.
length	Netmask length, in the range from 1 to 32.
local-tag *vpi vci*	Matches locally assigned label values.
neighbor atm *slot/subslot/port*	Matches labels assigned by a neighbor on the specified ATM interface.
remote-tag *vpi vci*	Matches remotely assigned label values.

Defaults

Displays all database entries.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced on the Cisco 6400 NSP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3	This command was integrated into Cisco IOS Release 12.3.

Usage Guidelines

The display output can show the entire database or a subset of entries based on the prefix, the VC label value, or an assigning interface.

Examples

The following is sample output from this command.

```
Switch#   show tag-switching atm-tdp bindings
Destination: 13.13.13.6/32
      Headend Router ATM1/0.1 (2 hops) 1/33 Active, VCD=8, CoS=available
      Headend Router ATM1/0.1 (2 hops) 1/34 Active, VCD=9, CoS=standard
          Headend Router ATM1/0.1 (2 hops) 1/35 Active, VCD=10, CoS=premium
              Headend Router ATM1/0.1 (2 hops) 1/36 Active, VCD=11, CoS=control

Destination: 102.0.0.0/8
      Headend Router ATM1/0.1 (1 hop) 1/37 Active, VCD=4, CoS=available
      Headend Router ATM1/0.1 (1 hop) 1/34 Active, VCD=5, CoS=standard
          Headend Router ATM1/0.1 (1 hop) 1/35 Active, VCD=6, CoS=premium
              Headend Router ATM1/0.1 (1 hop) 1/36 Active, VCD=7, CoS=control
```

Destination: 13.0.0.18/32
    Tailend Router ATM1/0.1 1/33 Active, VCD=8

Table 4-2 describes the significant fields in the sample command output shown above.

Table 4-2   Show Tag-switching Atm-tdp Bindings Field Descriptions

Field	Description
Destination:	Destination IP address/length of netmask
Headend Router	VC type: • Headend—VC that originates at this router • Tailend—VC that terminates at this router
ATM1/0.1	ATM interface
1/33	VPI/VCI
Active	LVC state: • Active—Set up and working • Bindwait—Waiting for response

Related Commands	Command	Description
	show tag-switching atm-tdp bindwait	Displays the number of bindings waiting for label assignments for a remote MPLS ATM switch.

show tag-switching atm-tdp bindings

T

V