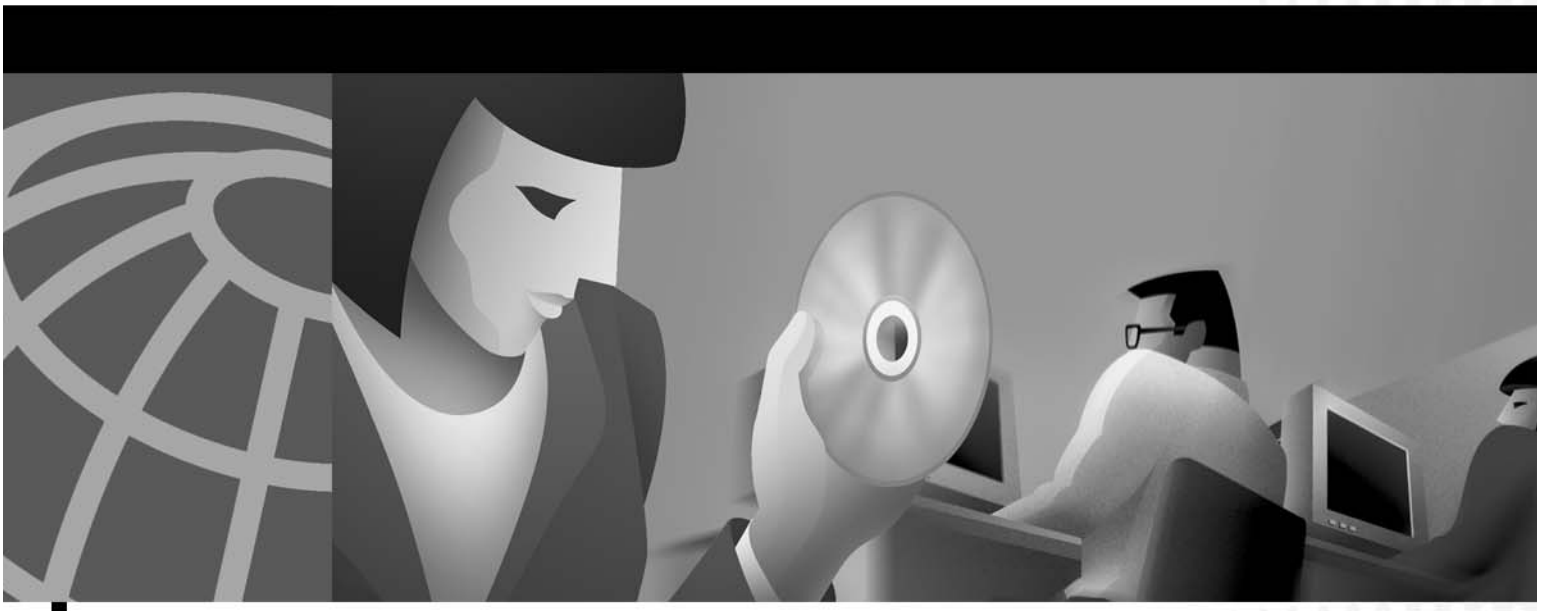


Cisco 6400 Feature Guide—Release 12.2(4)B

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

Text Part Number: OL-1800-01

CONTENTS

Preface

This chapter describes the objectives, organization, and audience of this guide, as well as conventions and related documentation.

Document Objectives

The objectives of this guide are to:

- Identify the software features supported by the Cisco 6400 carrier-class broadband aggregator in Cisco IOS Release 12.2(4)B
- Provide links to documentation for each feature
- Describe deployment of features that are unique to the Cisco 6400
- Supplement cross-platform feature information with information specific to the Cisco 6400, including descriptions, configuration and verification information, examples, prerequisites, and restrictions.

See the Supported Features chapter for a list of features supported by the Cisco 6400 in Cisco IOS Release 12.2(4)B. The Supported Features chapter also provides links to documentation for each feature. Some of the links go to other sections of this guide, while the rest of the links go to other documents available on Cisco.com.

Related Documentation

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

Document	Description
Cisco 6400 Software Setup Guide	Describes how to set up the Cisco 6400 with a basic configuration and connectivity among the Cisco 6400 components.
Cisco 6400 Command Reference	Describes commands that are unique to the Cisco 6400 command-line interface (CLI).

Document	Description
ATM Switch Router Software Configuration Guide	Describes additional ATM features and functionality that are supported by the Cisco 6400 node switch processor (NSP).
ATM and Layer 3 Switch Router Command Reference	Describes additional commands supported by the Cisco 6400 NSP.
Cisco IOS Configuration Guides and Command References	Describes extensive Cisco IOS features and commands that apply to the Cisco 6400.

Audience

This guide is designed for the system administrator who will be responsible for setting up the Cisco IOS software on the Cisco 6400. The system administrator should be familiar with the installation of high-end networking equipment.

This guide 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 Cisco IOS software
- System administrators who are responsible for installing and configuring internetworking equipment, and who are familiar with Cisco IOS software

Organization

The *Cisco 6400 Feature Guide* is organized into the following chapters and appendixes:

Chapter 1	Supported Features	Describes features supported in Cisco IOS Release 12.2(4)B and where to find feature information.
Chapter 2	Layer 2 Tunnel Protocol	Describes L2TP features.
Chapter 3	Multiprotocol Label Switching	Describes MPLS features.
Chapter 4	Point-to-Point Protocol	Describes PPP features.
Chapter 5	Session and Tunnel Scalability	Describes session and tunnel scalability parameters.
Chapter 6	Miscellaneous Features	Describes miscellaneous features.
Glossary	—	Provides technology definitions.

Conventions

This section describes the following conventions used by this guide:

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

Command Syntax

Descriptions of command syntax use the following conventions:

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

Examples use the following conventions:

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

This guide uses the following conventions for typing keys:

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, Cautions, and Warnings

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.

Warning **This warning symbol means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.**

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.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

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

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

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, 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 the **Fax** or **Email** option under the "Leave Feedback" at the bottom of the Cisco Documentation home page.

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 Web Site 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, 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 level 2; 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.

CHAPTER 1

Supported Features

This chapter lists the features supported by the Cisco 6400 carrier-class broadband aggregator in Cisco IOS Release 12.2(4)B and identifies feature documentation that you can find on Cisco.com.

The topics addressed are:

Conventions Used in This Chapter

Feature documentation publication names are in *italics*. When applicable, the path to the most useful section of the publication is provided in a bulleted list after the publication name. The bulleted items can be book part titles, chapter titles, section names, or subsection names.

Table 1-1 Examples of Conventions Used in the "Supported Features" Chapter

Feature	Documentation
RBE with DHCP	*Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*: • Configuring Broadband Access: PPP and Routed Bridge Encapsulation • Configuring ATM Routed Bridge Encapsulation *Cisco IOS IP Configuration Guide, Release 12.2*: • IP Addressing and Services • Configuring DHCP
RFC 1577	*Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*: • Configuring ATM • Configuring Classical IP and ARP over ATM

Node Route Processor Features

The Cisco 6400 supports three node route processors, designated as NRP-1, NRP-2, and NRP-2SV:

- NRP-1—Incorporates a 100-Mbps Fast Ethernet interface for connecting into an IP network and has processing capability for OC-3 rate of user traffic.
- NRP-2 and NRP-2SV—Provides a Gigabit Ethernet interface and sufficient processing capability for handling OC-12 rate of user traffic.

The Feature column states whether the NRP feature is supported by or applicable to only one or two types of NRP.

Access Protocols

Table 1-2 NRP Features—Access Protocols

Feature	Documentation
ATM VC Traffic Shaping (NRP-1 and NRP-2SV only)	*Cisco 6400 Software Setup Guide*: • Basic NRP Configuration • Configuring PVC Traffic Shaping
Enhancements to DHCP Option 82 Support for RBE	*Release Notes for Cisco 6400 for Cisco IOS Release 12.2(4)B*: • New and Changed Information • New Software Features Supported in Release 12.2(4)B • Enhancements to DHCP Option 82 Support for RBE *Cisco 6400 Feature Guide—Release 12.2(4)B*: • Miscellaneous Features • DHCP Option 82 Support for Routed Bridge Encapsulation
IRB[1]	*DSL Architecture: Reliablility Design Plan*: • DSL Network Architectures • Integrated Routing and Bridging (IRB)/RFC 1483 Bridging *Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2*: • Bridging
Multilink PPP	*Cisco IOS Dial Technologies Configuration Guide, Release 12.2*: • PPP Configuration • Configuring Media-Independent PPP and Multilink PPP
PPP IPCP[2] Subnet Negotiation	*Cisco IOS Dial Technologies Configuration Guide, Release 12.2*: • PPP Configuration • Configuring Asynchronous SLIP and PPP • Configuring Network-Layer Protocols over PPP and SLIP *Cisco 6400 Feature Guide—Release 12.2(4)B*: • Miscellaneous Features • IPCP Subnet Mask Support
PPPoA[3] terminated	*Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*: • Configuring Broadband Access: PPP and Routed Bridge Encapsulation • Configuring PPP over ATM *Cisco 6400 Feature Guide—Release 12.2(4)B*: • Point-to-Point Protocol • Configuring PPPoA *PPPoA Baseline Architecture*, white paper

Table 1-2 NRP Features—Access Protocols (continued)

Feature	Documentation
PPPoE[4] terminated	*Cisco 6400 Feature Guide—Release 12.2(4)B*: • Point-to-Point Protocol • Configuring PPPoE *Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*: • Configuring Broadband Access: PPP and Routed Bridge Encapsulation *PPPoE Baseline Architecture for the Cisco 6400 UAC*, white paper
PPPoA/PPPoE autosense on ATM VC with SNAP[5] encapsulation (Previously called "PPP autosense (SNAP)")	*Cisco 6400 Feature Guide—Release 12.2(4)B*: • Point-to-Point Protocol • Configuring PPPoA/PPPoE Autosense
PPPoE over Ethernet (FE for NRP-1, GE for NRP-2SV only)	*Cisco IOS Wide-Area Networking Configuration Guide:* • Configuring Broadband Access: PPP and Routed Bridge Encapsulation • Configuring PPPoE over Ethernet
PPPoE over Ethernet with VLAN (NRP-1 and NRP-2SV only)	*Release Notes for Cisco 6400 for Cisco IOS Release 12.2(4)B*: • New and Changed Information • New Software Features Supported in Release 12.2(4)B • PPPoE over Ethernet with VLAN *Cisco IOS Wide-Area Networking Configuration Guide:* • Configuring Broadband Access: PPP and Routed Bridge Encapsulation • Configuring PPPoE over Ethernet *Cisco IOS Switching Services Configuration Guide, Release 12.2*: • Virtual LANs
RBE[6]	*Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*: • Configuring Broadband Access: PPP and Routed Bridge Encapsulation • Configuring ATM Routed Bridge Encapsulation *DSL Architecture: Reliablility Design Plan*: • DSL Network Architectures • Routed Bridge Encapsulation (RBE)
RBE Subinterface Grouping	*Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*: • Configuring Broadband Access: PPP and Routed Bridge Encapsulation • Configuring ATM Routed Bridge Encapsulation • ATM RBE Subinterface Grouping by PVC Range

Table 1-2 NRP Features—Access Protocols (continued)

Feature	Documentation
RBE unnumbered DHCP[7]	*Release Notes for Cisco 6400 NRP for Cisco IOS Release 12.1(1) DC1*: • New and Changed Information • New Software Features in Release 12.1(1) DC1 • Dynamic Host Configuration Protocol Relay for Unnumbered Interfaces Using ATM RBE *Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*: • Configuring Broadband Access: PPP and Routed Bridge Encapsulation • Configuring ATM Routed Bridge Encapsulation *Cisco IOS IP Configuration Guide, Release 12.2*: • IP Addressing and Services • Configuring DHCP
RBE with DHCP	*Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*: • Configuring Broadband Access: PPP and Routed Bridge Encapsulation • Configuring ATM Routed Bridge Encapsulation *Cisco IOS IP Configuration Guide, Release 12.2*: • IP Addressing and Services • Configuring DHCP
RBE with DHCP Option 82	*Cisco 6400 Feature Guide—Release 12.2(4)B*: • Miscellaneous Features • DHCP Option 82 Support for Routed Bridge Encapsulation
RFC 1483 bridging	*DSL Architecture: Reliablility Design Plan*: • DSL Network Architectures • Integrated Routing and Bridging (IRB)/RFC 1483 Bridging *Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2*: • Bridging *Cisco 6400 NRP Configuration and Troubleshooting*, white paper *Basic PVC Configuration Using Bridged RFC 1483*, sample configuration
RFC 1483 routing	*Cisco IOS IP Configuration Guide, Release 12.2*: • IP Routing Protocols *Cisco 6400 NRP Configuration and Troubleshooting*, white paper

1. IRB = integrated routing and bridging
2. IPCP = IP Control Protocol
3. PPPoA = PPP over ATM
4. PPPoE = PPP over Ethernet
5. SNAP = Subnetwork Access Protocol
6. RBE = Routed Bridge Encapsulation
7. DHCP = Dynamic Host Configuration Protocol

Aggregation and Virtual Private Networks (VPNs)

Table 1-3 NRP Features—Aggregation and VPNs

Feature	Documentation
DHCP Relay Support for MPLS VPN Suboptions	*DHCP Relay Support for MPLS VPN Suboptions*, 12.2(4)B feature module
IP Overlapping Address Pools (NRP-1 only)	*Cisco 6400 Feature Guide—Release 12.2(4)B*: • Miscellaneous Features • IP Overlapping Address Pools
L2TP[1] Multi-Hop	*Multihop VPDN*, 11.3(3)T feature module *Configuring L2TP Multihop to Perform Several Hops from the NAS to the LNS*, Sample Configuration
L2TP remote access into MPLS[2] VPN[3]	Cisco Remote Access to MPLS VPN Solution 1.0 documentation *Cisco 6400 Feature Guide—Release 12.2(4)B*: • Multiprotocol Label Switching • Configuring MPLS Virtual Private Networks *Cisco IOS Switching Services Configuration Guide, Release 12.2*: • Multiprotocol Label Switching
L2TP tunnel service authorization enhancement	*Cisco 6400 Feature Guide—Release 12.2(4)B*: • Layer 2 Tunnel Protocol • Tunnel Service Authorization Enhancements
L2TP tunnel sharing	*Cisco 6400 Feature Guide—Release 12.2(4)B*: • Layer 2 Tunnel Protocol • Tunnel Sharing
L2TP tunnel switching	*Cisco 6400 Feature Guide—Release 12.2(4)B*: • Layer 2 Tunnel Protocol • Tunnel Switching
MPLS Edge LSR[4]	*Cisco 6400 Feature Guide—Release 12.2(4)B*: • Multiprotocol Label Switching
MPLS LDP[5]	*MPLS Label Distribution Protocol*, 12.2(2)T feature module
MPLS LSC[6] for BPX	*Cisco IOS Switching Services Configuration Guide, Release 12.2*: • Multiprotocol Label Switching
MPLS VPNs	*Cisco 6400 Feature Guide—Release 12.2(4)B*: • Multiprotocol Label Switching • Configuring MPLS Virtual Private Networks *Cisco IOS Switching Services Configuration Guide, Release 12.2*: • Multiprotocol Label Switching
MPLS VPN ID	*MPLS VPN ID* , 12.2(4)B feature module

Table 1-3 NRP Features—Aggregation and VPNs (continued)

Feature	Documentation
PPPoA tunneled into L2TP	*Cisco 6400 Feature Guide—Release 12.2(4)B*: • Layer 2 Tunnel Protocol *Cisco 6400 Feature Guide—Release 12.2(4)B*: • Point-to-Point Protocol • Configuring PPPoA *Layer 2 Tunneling Protocol*, fact sheet
PPPoE tunneled into L2TP	*Cisco 6400 Feature Guide—Release 12.2(4)B*: • Layer 2 Tunnel Protocol *Cisco 6400 Feature Guide—Release 12.2(4)B*: • Point-to-Point Protocol • Configuring PPPoE *Layer 2 Tunneling Protocol*, fact sheet
PPPoA/PPPoE remote access into MPLS VPN	Cisco Remote Access to MPLS VPN Solution 1.0 documentation *Cisco 6400 Feature Guide—Release 12.2(4)B*: • Multiprotocol Label Switching • Configuring MPLS Virtual Private Networks *Cisco IOS Switching Services Configuration Guide, Release 12.2*: • Multiprotocol Label Switching
RBE remote access into MPLS VPN (NRP-1 only)	Cisco Remote Access to MPLS VPN Solution 1.0 documentation *Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*: • Configuring Broadband Access: PPP and Routed Bridge Encapsulation • Configuring ATM Routed Bridge Encapsulation
RFC 1577	*Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*: • Configuring ATM • Configuring Classical IP and ARP over ATM
Session Limit Per VRF	*Session Limit Per VRF*, 12.2(4)B feature module
SSG remote access into MPLS VPN (Two-card solution)	Cisco Remote Access to MPLS VPN Solution 1.0 documentation SSG Features in Release 12.2(4)B
VLAN (ISL[7]) on NRP	*Cisco IOS Switching Services Configuration Guide, Release 12.2*: • Virtual LANs • Configuring Routing Between VLANs with ISL Encapsulation
VLAN (802.1q) on GE[8] (NRP-2 and NRP-2SV only)	*Cisco IOS Switching Services Configuration Guide, Release 12.2*: • Virtual LANs • Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation

1. L2TP = Layer 2 Tunnel Protocol
2. MPLS = Multiprotocol Label Switching

3. VPN = Virtual Private Network
4. LSR = label switch router
5. LDP = label distribution protocol
6. LSC = label switch controller
7. ISL = Inter-Switch Link
8. GE = Gigabit Ethernet

Configuration and Monitoring

Table 1-4 NRP Features—Configuration and Monitoring

Feature	Documentation
ATM OAM Ping	*ATM OAM Ping*, 12.2(4)B feature module
ATM PVC[1] Range	*Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*: • Configuring Broadband Access: PPP and Routed Bridge Encapsulation • Configuring an ATM PVC Range
Per VC[2] error display	*Cisco 6400 Command Reference*: • Show Commands for the Cisco 6400 NRP • show controllers atm 0/0/0

1. PVC = permanent virtual circuit (or connection)
2. VC = virtual circuit (or connection)

Hardware Support

Table 1-5 NRP Features—Hardware Support

Feature	Documentation
FE[1] Interface (10/100 auto-negotiation, auto-sensing) (NRP-1 only)	*Cisco IOS Interface Configuration Guide, Release 12.2*: • Configuring LAN Interfaces • Configuring Ethernet, Fast Ethernet, or Gigabit Ethernet Interfaces
GE Interface (NRP-2 and NRP-2SV only)	*Gigabit Ethernet Port Adapter*, 12.1(4)E feature module
NME[2]	*Cisco 6400 Software Setup Guide*: • Basic NSP Configuration • Network Management Ethernet Interface • Enabling NME Consolidation on the NRP
NRP 1+1 Redundancy (NRP-1 only)	*Cisco 6400 Software Setup Guide*: • Redundancy and SONET APS Configuration • NRP Redundancy

1. FE = Fast Ethernet
2. NME = Network Management Ethernet

IP and Routing

Table 1-6 NRP Features—IP and Routing

Feature	Documentation
ARP[1]	*Cisco IOS IP Configuration Guide, Release 12.2*: • IP Addressing and Services • Configuring IP Addressing • Configuring Address Resolution Methods
BGP4[2]	*Cisco IOS IP Configuration Guide, Release 12.2*: • IP Routing Protocols • Configuring BGP
EIGRP[3]	*Cisco IOS IP Configuration Guide, Release 12.2*: • IP Routing Protocols • Configuring IP Enhanced IGRP
GRE[4]	*Cisco IOS Interface Configuration Guide, Release 12.2*: • Configuring Logical Interfaces • Configuring a Tunnel Interface
IGMP[5]	*Cisco IOS IP Configuration Guide, Release 12.2*: • IP Multicast • Configuring IP Multicast Routing • IGMP Features Configuration Task List
IP forwarding	*Cisco IOS IP Configuration Guide, Release 12.2*: • IP Addressing and Services • Configuring IP Services
IP multicast	*Cisco IOS IP Configuration Guide, Release 12.2*: • IP Multicast *Internet Protocol (IP) Multicast Technology Overview*, white paper
IS-IS[6]	*Cisco IOS IP Configuration Guide, Release 12.2*: • IP Routing Protocols • Configuring Integrated IS-IS
NAT[7] support for NetMeeting Directory	*Cisco IOS IP Configuration Guide, Release 12.2*: • IP Addressing and Services • Configuring IP Addressing • Configuring Network Address Translation

Table 1-6 NRP Features—IP and Routing (continued)

Feature	Documentation
NetFlow for RFC 1483 into MPLS VPN (NRP- 1 only)	*Cisco IOS Switching Services Configuration Guide, Release 12.2*: • NetFlow Switching *Cisco 6400 Feature Guide—Release 12.2(4)B*: • Multiprotocol Label Switching • Configuring MPLS Virtual Private Networks *Cisco IOS Technical Marketing NetFlow Deployment on Logical Interfaces*, white paper
OSPF[8]	*Cisco IOS IP Configuration Guide, Release 12.2*: • IP Routing Protocols • Configuring OSPF
PIM[9] Dense Mode & Sparse Mode	*Cisco IOS IP Configuration Guide, Release 12.2*: • IP Multicast • Configuring IP Multicast Routing
RIP[10] (Version 1 and Version 2)	*Cisco IOS IP Configuration Guide, Release 12.2*: • IP Routing Protocols • Configuring Routing Information Protocol
TCP[11]	*Cisco IOS IP Configuration Guide, Release 12.2*: • IP Overview
Telnet	*Cisco IOS Terminal Services Configuration Guide, Release 12.2*: • Configuring Dial-In Terminal Services • Telnet and rlogin Configuration Task List
TFTP	*Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*: • File Management • Configuring Basic File Transfer Services • Configuring a Router as a TFTP or RARP Server
Transparent Bridging	*Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2*: • Bridging • Configuring Transparent Bridging
UDP[12]	*Internetworking Technology Overview*: • Internet Protocols (IP) • Transmission Control Protocol (TCP) • User Datagram Protocol (UDP)
WCCP[13] (v1 and v2)	*Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*: • System Management • Configuring Web Cache Services Using WCCP

1. ARP = Address Resolution Protocol

2. BGP4 = Border Gateway Protocol Version 4
3. EIGRP = Enhanced Interior Gateway Routing Protocol
4. GRE = generic routing encapsulation
5. IGMP = Internet Group Management Protocol
6. IS-IS = Intermediate System-to-Intermediate System
7. NAT = Network Address Translation
8. OSPF = Open Shortest Path First
9. PIM = Protocol Independent Multicast
10. RIP = Routing Information Protocol
11. TCP = Transmission Control Protocol
12. UDP = User Datagram Protocol
13. WCCP = Web Cache Communication Protocol

Network Management

Table 1-7 NRP Features—Network Management

Feature	Documentation
ATM SNMP[1] trap and OAM[2] enhancements	*Cisco 6400 Feature Guide—Release 12.2(4)B*: • Miscellaneous Features • ATM SNMP Trap and OAM Enhancements
PPPoE session count MIB	*Cisco 6400 Feature Guide—Release 12.2(4)B*: • Point-to-Point Protocol • Configuration Tasks • Configuring PPPoE Session Count MIB
SNMP (v1 and v2)	*Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*: • System Management • Configuring SNMP Support
SNMPv3 (NRP-2 and NRP-2SV only)	*Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2*: • System Management • Configuring SNMP Support *Cisco 6400 Software Setup Guide*: • SNMP, RMON, and Alarm Configuration • Using the NSP as the SNMPv3 Proxy Forwarder for the NRP-2

1. SNMP = Simple Network Management Protocol
2. OAM = Operation, Administration, and Maintenance

QoS

Table 1-8 NRP Features—QoS

Feature	Documentation
IP QoS—Policing, Marking, and Classification	*Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2*: • Policing and Shaping

RADIUS/AAA

Table 1-9 NRP Features—RADIUS/AAA

Feature	Documentation
Encrypted and Tagged VSA Support for RADIUS Attribute 91	*Release Notes for Cisco 6400 for Cisco IOS Release 12.2(4)B*: • New and Changed Information • New Software Features Supported in Release 12.2(4)B • Encrypted and Tagged VSA Support for RADIUS Attribute 91
Enhancements to RADIUS VC Logging	*Release Notes for Cisco 6400 for Cisco IOS Release 12.2(4)B*: • New and Changed Information • New Software Features Supported in Release 12.2(4)B • Enhancements to RADIUS VC Logging *Cisco 6400 Feature Guide—Release 12.2(4)B*: • Miscellaneous Features • RADIUS VC Logging
Extended Support for RADIUS Attribute 32	*Release Notes for Cisco 6400 for Cisco IOS Release 12.2(4)B*: • New and Changed Information • New Software Features Supported in Release 12.2(4)B • Extended Support for RADIUS Attribute 32
Framed Route VRF Aware	*Release Notes for Cisco 6400 for Cisco IOS Release 12.2(4)B*: • New and Changed Information • New Software Features Supported in Release 12.2(4)B • Framed Route VRF Aware
IETF[1] Tunnel Attributes	*Cisco IOS Security Configuration Guide, Release 12.2*: • Security Server Protocols • Configuring RADIUS • RADIUS Attributes

Table 1-9 NRP Features—RADIUS/AAA (continued)

Feature	Documentation
PAP[2]/CHAP[3]	*Cisco IOS Security Configuration Guide, Release 12.2*: • Authentication, Authorization, and Accounting (AAA) • Configuring Authentication • Non-AAA Authentication Methods • Enabling CHAP or PAP Authentication
Per VRF AAA	*Per VRF AAA*, 12.2(4)B feature module
RADIUS	*Cisco IOS Security Configuration Guide, Release 12.2*: • Security Server Protocols • Configuring RADIUS
RADIUS Attribute 8 (Framed-IP-Address) in Access Requests (IP Hint)	*RADIUS Attribute 8 (Framed-IP-Address) in Access Requests*, 12.1(5)T feature module
RADIUS-based Session/Idle Timeout for LAC	*Release Notes for Cisco 6400 for Cisco IOS Release 12.2(4)B*: • New and Changed Information • New Software Features Supported in Release 12.2(4)B • RADIUS-based Session/Idle Timer for L2TP LAC
Support for RADIUS Attributes 52 and 53	*Release Notes for Cisco 6400 for Cisco IOS Release 12.2(4)B*: • New and Changed Information • New Software Features Supported in Release 12.2(4)B • Support for RADIUS Attributes 52 and 53
Support for RADIUS Attribute 77	*Release Notes for Cisco 6400 for Cisco IOS Release 12.2(4)B*: • New and Changed Information • New Software Features Supported in Release 12.2(4)B • Support for RADIUS Attribute 77
TACACS+ (admin login only)	*Cisco IOS Security Configuration Guide, Release 12.2*: • Security Server Protocols • Configuring TACACS+
VPI[4]/VCI[5] in RADIUS Request/Accounting for PPPoA	*Cisco 6400 Feature Guide—Release 12.2(4)B*: • Miscellaneous Features • RADIUS VC Logging
VPI/VCI in RADIUS Request/Accounting for PPPoE	*Cisco 6400 Feature Guide—Release 12.2(4)B*: • Miscellaneous Features • RADIUS VC Logging

1. IETF = Internet Engineering Task Force
2. PAP = Password Authentication Protocol
3. CHAP = Challenge Handshake Authentication Protocol
4. VPI = virtual path identifier

5. VCI = virtual channel identifier

Scalability and Performance

Table 1-10 NRP Features—Scalability and Performance

Feature	Documentation
GRE CEF[1]	*Cisco IOS Switching Services Configuration Guide, Release 12.2*: • Cisco IOS Switching Paths *Cisco IOS Interface Configuration Guide, Release 12.2*: • Configuring Logical Interfaces • Configuring a Tunnel Interface
L2TP sessions per tunnel limiting	*Cisco 6400 Feature Guide—Release 12.2(4)B*: • Layer 2 Tunnel Protocol • Configuring L2TP • Sessions per Tunnel Limiting
LAC CEF switching	*Cisco IOS Switching Services Configuration Guide, Release 12.2*: • Cisco IOS Switching Paths *Cisco 6400 Feature Guide—Release 12.2(4)B*: • Layer 2 Tunnel Protocol • Configuring L2TP • Configuring VPDN on the LAC *Layer 2 Tunneling Protocol*, fact sheet
NAT CEF switched	*Cisco IOS Switching Services Configuration Guide, Release 12.2*: • Cisco IOS Switching Paths *Cisco IOS IP Configuration Guide, Release 12.2*: • IP Addressing and Services • Configuring IP Addressing • Configuring Network Address Translation
Per VC buffer management	*Cisco 6400 Software Setup Guide*: • Basic NRP Configuration • NRP-1 Configuration • Segmentation and Reassembly Buffer Management
PPPoA CEF	*Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*: • Configuring Broadband Access: PPP and Routed Bridge Encapsulation • Configuring PPP over ATM *Cisco IOS Switching Services Configuration Guide, Release 12.2*: • Cisco IOS Switching Paths

Table 1-10 NRP Features—Scalability and Performance (continued)

Feature	Documentation
PPPoE Fast Switched for Multicast	*Cisco IOS Dial Technologies Configuration Guide, Release 12.2*: • PPP Configuration • Configuring Asynchronous SLIP and PPP
PPPoE Session Limit (per ATM VC)	*PPPoE Session Limit*, 12.2(4)T feature module
RBE CEF	*Cisco IOS Switching Services Configuration Guide, Release 12.2*: • Cisco IOS Switching Paths *Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*: • Configuring Broadband Access: PPP and Routed Bridge Encapsulation • Configuring ATM Routed Bridge Encapsulation *DSL Architecture: Reliablility Design Plan*: • DSL Network Architectures • Routed Bridge Encapsulation (RBE)

1. CEF = Cisco Express Forwarding

Service Selection Gateway (SSG)

Table 1-11 NRP Features—SSG

Feature	Documentation
PTA[1] Multi-Domain	*Service Selection Gateway*, 12.2(4)B feature module: • Feature Overview • Multiple Traffic-Type Support • PPP Termination Aggregation (PTA) and PTA Multi-Domain (PTA-MD)
RADIUS Interim Accounting	*Service Selection Gateway*, 12.2(4)B feature module: • Configuring SSG Features • Configuring RADIUS Interim Accounting
SSG AAA[2] Server Group Support for Proxy RADIUS	*Service Selection Gateway*, 12.2(4)B feature module: • Configuring RADIUS Profiles • Service Profiles • RADIUS Server
SSG Accounting Update Interval Per Service	*Service Selection Gateway Accounting Update Interval Per Service*, 12.2(4)B feature module
SSG AutoDomain	*SSG AutoDomain*, 12.2(4)B feature module
SSG Autologoff	*SSG Autologoff*, 12.2(4)B feature module
SSG AutoLogon Using Proxy RADIUS	*SSG AutoLogon Using Proxy RADIUS*, 12.2(4)B feature module

Table 1-11 NRP Features—SSG (continued)

Feature	Documentation
SSG Automatic Service Logon	*Service Selection Gateway*, 12.2(4)B feature module: • Configuring RADIUS Profiles • User Profiles • Auto Service
SSG CEF Switched	*Service Selection Gateway*, 12.2(4)B feature module: • Configuring SSG Features • Configuring Cisco Express Forwarding
SSG Cisco IOS NAT	*Service Selection Gateway*, 12.2(4)B feature module: • Configuring SSG Features • Configuring Cisco IOS Network Address Translation
SSG Default Network	*Service Selection Gateway*, 12.2(4)B feature module: • Configuring SSG Features • Configuring a Default Network
SSG DNS[3] Selection and Fault Tolerance	*Service Selection Gateway*, 12.2(4)B feature module: • Configuring RADIUS Profiles • Service Profiles • DNS Server Address
SSG enable (default is disabled)	*Service Selection Gateway*, 12.2(4)B feature module: • Configuring SSG Features • Enabling SSG
SSG full username RADIUS attribute	*Service Selection Gateway*, 12.2(4)B feature module: • Configuring RADIUS Profiles • Service Profiles • Full Username
SSG Hierarchical Policing	*Service Selection Gateway Hierarchical Policing*, 12.2(4)B feature module
SSG Host Key	*SSG Port-Bundle Host Key*, 12.2(4)B feature module:
SSG Local Forwarding	*Service Selection Gateway*, 12.2(4)B feature module: • Configuring SSG Features • Configuring Local Forwarding
SSG Open Garden	*Service Selection Gateway*, 12.2(4)B feature module: • Configuring SSG Features • Configuring an Open Garden

Table 1-11 NRP Features—SSG (continued)

Feature	Documentation
SSG Passthrough and Proxy Service	*Service Selection Gateway*, 12.2(4)B feature module: • Configuring RADIUS Profiles • Service Profiles • Type of Service
SSG Prepaid Billing	*SSG Prepaid*, 12.2(4)B feature module
SSG Sequential and Concurrent Service	*Service Selection Gateway*, 12.2(4)B feature module: • Configuring RADIUS Profiles • Service Profiles • Service Mode
SSG Service Defined Cookie	*Service Selection Gateway*, 12.2(4)B feature module: • Configuring RADIUS Profiles • Service Profiles • Service-Defined Cookie
SSG single host logon	*Service Selection Gateway*, 12.2(4)B feature module: • Feature Overview • SSG Single Host Logon
SSG Support for MAC Addresses in Accounting Records	*Release Notes for Cisco 6400 for Cisco IOS Release 12.2(4)B*: • New and Changed Information • New Software Features Supported in Release 12.2(4)B • SSG Support for MAC Addresses in Accounting Records
SSG TCP Redirect for Services (Previously called “SSG HTTP Redirect” and “SSG TCP Redirect - Logon”)	*SSG TCP Redirect for Services*, 12.2(4)B feature module
SSG with GRE	*Cisco IOS Interface Configuration Guide, Release 12.2*: • Configuring Logical Interfaces • Configuring a Tunnel Interface *Service Selection Gateway*, 12.2(4)B feature module
SSG with L2TP Service Type	*Service Selection Gateway*, 12.2(4)B feature module: • Configuring SSG Features • Configuring SSG to Support L2TP Service Type
VPI/VCI Static binding to a Service Profile	*Service Selection Gateway*, 12.2(4)B feature module: • Configuring SSG Features • Configuring VPI/VCI Indexing to Service Profile
WebSelection	*Service Selection Gateway*, 12.2(4)B feature module Cisco Subscriber Edge Services Manager documentation Cisco Service Selection Dashboard documentation

1. PTA = PPP Termination Aggregation
2. AAA = authentication, authorization, and accounting
3. DNS = Domain Name System

Other Features and Feature Enhancements

Table 1-12 NRP Features—Other Features and Feature Enhancements

Feature	Documentation
Segmentation and Reassembly Buffer Management Enhancements (NRP-1 only)	*Cisco 6400 Software Setup Guide*: • Basic NRP Configuration • NRP-1 Configuration • Segmentation and Reassembly Buffer Management

Node Switch Processor Features

The Node Switch Processor (NSP) contains the ATM switch engine and processor, and most memory components.

Aggregation and Virtual Private Networks (VPNs)

Table 1-13 NSP Features—Aggregation and VPNs

Feature	Documentation
MPLS ATM LSR[1]	*ATM Switch Router Software Configuration Guide*: • Configuring Tag Switching

1. LSR = label switch router

ATM Connections

Table 1-14 NSP Features—ATM Connections

Feature	Documentation
F4 and F5 OAM[1] cell segment and end-to-end flows	*ATM Switch Router Software Configuration Guide*: • Configuring Operation, Administration, and Maintenance
Hierarchical VP[2] tunnels	*ATM Switch Router Software Configuration Guide*: • Configuring Virtual Connections • Configuring VP Tunnels • Configuring a Hierarchical VP Tunnel for Multiple Service Categories

Table 1-14 NSP Features—ATM Connections (continued)

Feature	Documentation
Logical multicast support (up to 254 leaves per output port, per point-to-multipoint VC)	*ATM Switch Router Software Configuration Guide*: • Configuring Virtual Connections • Configuring Point-to-Multipoint PVC Connections
Multipoint-to-point UNI[3] signaling	*Cisco 6400 Software Setup Guide*: • Node Line Card Interface Configuration • ATM Interface Types • User-Network Interfaces
Point-to-Point and Point-to-Multipoint VCs	*ATM Switch Router Software Configuration Guide*: • Configuring Virtual Connections
PVC[4], Soft PVC, Soft PVP[5], and SVC[6]	*ATM Switch Router Software Configuration Guide*: • Configuring Virtual Connections
Soft VCCs[7] and VPCs[8]	*ATM Switch Router Software Configuration Guide*: • Configuring Virtual Connections
VC Merge	*ATM Switch Router Software Configuration Guide*: • Configuring Tag Switching • Configuring VC Merge
VP and VC switching	*Cisco 6400 Software Setup Guide*: • Basic NSP Configuration • Internal Cross-Connections
VP multiplexing	*Understanding VP Tunnels and VP Switching*, tech note
VP tunneling	*ATM Switch Router Software Configuration Guide*: • Configuring Virtual Connections • Configuring VP Tunnels

1. OAM = Operation, Administration, and Maintenance
2. VP = virtual path
3. UNI = User-Network Interface
4. PVC = permanent virtual circuit (or connection)
5. PVP = permanent virtual path
6. SVC = switched virtual circuit
7. VCC = virtual channel connection
8. VPC = virtual path connection

ATM Internetworking

Table 1-15 NSP Features—ATM Internetworking

Feature	Documentation
LES[1] and LECS[2]	*ATM Switch Router Software Configuration Guide*: • Configuring LAN Emulation
RFC 1577 (Classical IP over ATM) ATM ARP[3] server/client	*ATM Switch Router Software Configuration Guide*: • Configuring IP over ATM • Configuring Classical IP over ATM

1. LES = LAN Emulation Server
2. LECS = LAN Emulation Configuration Server
3. ARP = Address Resolution Protocol

ATM Per-Flow Queuing

Table 1-16 NSP Features—ATM Per-Flow Queuing

Feature	Documentation
Dual leaky bucket policing (ITU-T I.371 and ATM Forum UNI specifications)	*Guide to ATM Technology*: • Traffic and Resource Management • UPC—Traffic Policing at a Network Boundary *ATM Switch Router Software Configuration Guide*: • Configuring Resource Management • Processor Feature Card Functionality[1]
Intelligent EPD[2]	*ATM Switch Router Software Configuration Guide*: • Configuring Resource Management • Configuring Physical Interfaces • Configuring the Interface Queue Thresholds per Service Category *ATM and Layer 3 Switch Router Command Reference*: • ATM Commands • atm output-threshold *LightStream 1010 Switch Architecture and Traffic Management*, white paper
Intelligent partial (tail) packet discard	*ATM Switch Router Software Configuration Guide*: • Configuring Resource Management • Configuring Physical Interfaces • Configuring the Interface Queue Thresholds per Service Category *LightStream 1010 Switch Architecture and Traffic Management*, white paper

Table 1-16 NSP Features—ATM Per-Flow Queuing (continued)

Feature	Documentation
Multiple, weighted (dynamic) thresholds for selective packet marking and discard	*ATM Switch Router Software Configuration Guide*: • Configuring Resource Management • Processor Feature Card Functionality[1]
Per-VC or per-VP output queuing	*ATM Switch Router Software Configuration Guide*: • Configuring Resource Management • Processor Feature Card Functionality[1]
Strict priority, rate, or weighted round robin scheduling algorithms	*ATM Switch Router Software Configuration Guide*: • Configuring Resource Management • Configuring Physical Interfaces • Configuring the Scheduler and Service Class

1. The NSP uses the FC-PFQ feature card.
2. EPD = early packet discard

ATM Traffic Classes

Table 1-17 NSP Features—ATM Traffic Classes

Feature	Documentation
ABR[1] (EFCI[2] + RR[3]) + MCR[4]	*ATM Switch Router Software Configuration Guide*: • Configuring Resource Management • Configuring Physical Interfaces • Configuring the Interface Queue Thresholds per Service Category
CBR[5]	*ATM Switch Router Software Configuration Guide*: • Configuring Resource Management • Configuring Global Resource Management
Per-VC or per-VP CBR traffic shaping	*ATM Switch Router Software Configuration Guide*: • Configuring Resource Management • Configuring Global Resource Management[6]
Shaped CBR VP tunnels (up to 128 shaped tunnels)	*ATM Switch Router Software Configuration Guide*: • Configuring Resource Management • Configuring Global Resource Management[6]
Substitution of other service categories in shaped VP tunnels	*ATM Switch Router Software Configuration Guide*: • Configuring Resource Management • Configuring Physical and Logical Interface Parameters • Configuring Interface Service Category Support

Table 1-17 NSP Features—ATM Traffic Classes (continued)

Feature	Documentation
Support for non-zero MCR on ABR connections	*ATM Switch Router Software Configuration Guide*: • Configuring Resource Management • Configuring Physical Interfaces • Configuring the Interface Queue Thresholds per Service Category[6]
UBR[7]	*ATM Switch Router Software Configuration Guide*: • Configuring Resource Management • Configuring Global Resource Management[6]
UBR + MCR	*ATM Switch Router Software Configuration Guide*: • Configuring Resource Management • Configuring Global Resource Management • Configuring the Connection Traffic Table • CTT Supported Features
VBR-nrt[8]	*ATM Switch Router Software Configuration Guide*: • Configuring Resource Management • Configuring Global Resource Management[6]
VBR-rt[9]	*ATM Switch Router Software Configuration Guide*: • Configuring Resource Management • Configuring Global Resource Management[6]

1. ABR = available bit rate
2. EFCI = Explicit Forward Congestion Indication
3. RR = relative rate
4. MCR = minimum cell rate
5. CBR = constant bit rate
6. The NSP uses the FC-PFQ feature card.
7. UBR = unspecified bit rate
8. VBR-nrt = variable bit rate, non-real time
9. VBR-rt = variable bit rate, real time

Configuration and Monitoring

Table 1-18 NSP Features—Configuration and Monitoring

Feature	Documentation
ATM access lists on ILMI[1] registration	*ATM Switch Router Software Configuration Guide*: • Using Access Control • Configuring Per-Interface Address Registration with Optional Access Filters
ATM soft restart	*Cisco IOS Release 11.2(8.0.1) Release Notes for LightStream 1010 ATM Switch Software*: • New Release 11.2(8.0.1)FWA4(1) Features • ATM soft restart
PCMCIA[2] Disk Mirroring	*Cisco 6400 Software Setup Guide*: • Redundancy and SONET APS Configuration • NSP Redundancy • PCMCIA Disk Mirroring
Per-VC or per-VP nondisruptive port snooping	*ATM Switch Router Software Configuration Guide*: • Configuring Virtual Connections • Configuring Interface and Connection Snooping • Configuring Per-Connection Snooping

1. ILMI = Interim Local Management Interface
2. PCMCIA = Personal Computer Memory Card International Association

Hardware Support

Table 1-19 NSP Features—Hardware Support

Feature	Documentation
1+1 Slot Redundancy (EHSA[1])	*Cisco 6400 Software Setup Guide*: • Redundancy and SONET APS Configuration
ATM DS3, OC-3, and OC-12 node line cards	*Cisco 6400 Software Setup Guide*: • Node Line Card Interface Configuration
NME[2]	*Cisco 6400 Software Setup Guide*: • Basic NSP Configuration • Network Management Ethernet Interface
NRP-1 and NRP-2 support	*Cisco 6400 Software Setup Guide*: • Basic NSP Configuration

Table 1-19 NSP Features—Hardware Support (continued)

Feature	Documentation
NSP 1+1 Redundancy	*Cisco 6400 Software Setup Guide*: • Redundancy and SONET APS Configuration • NSP Redundancy
SONET APS[3]	*Cisco 6400 Software Setup Guide*: • Redundancy and SONET APS Configuration • SONET APS for NLC Port Redundancy
Stratum 3/BITS[4]	*Cisco 6400 Software Setup Guide*: • Basic NSP Configuration • Network Clocking • Configuring Building Integrated Timing Supply Network Clocking
Telco alarms	*Cisco 6400 Software Setup Guide*: • SNMP, RMON, and Alarm Configuration • Alarms

1. EHSA = enhanced high system availability
2. NME = Network Management Ethernet
3. APS = automatic protection switching
4. BITS = building integrated timing supply

IP and Routing

Table 1-20 NSP Features—IP and Routing

Feature	Documentation
DHCP[1] client support	*Cisco IOS IP Configuration Guide, Release12.2*: • IP Addressing and Services • Configuring DHCP
IP	*ATM Switch Router Software Configuration Guide*: • Configuring IP over ATM
NTP[2]	*ATM Switch Router Software Configuration Guide*: • Configuring System Management Functions • Configuring the Network Time Protocol
Telnet	*Cisco IOS Terminal Services Configuration Guide, Release 12.2*: • Configuring Dial-In Terminal Services • Telnet and rlogin Configuration Task List

1. DHCP = Dynamic Host Configuration Protocol
2. NTP = Network Time Protocol

Network Management

Table 1-21 NSP Features—Network Management

Feature	Documentation
ATM accounting enhancements	*ATM Switch Router Software Configuration Guide*: • Configuring ATM Accounting and ATM RMON
ATM Accounting MIB	*ATM Switch Router Software Configuration Guide*: • Configuring ATM Accounting and ATM RMON
ATM RMON[1] MIB	*ATM Switch Router Software Configuration Guide*: • Configuring ATM Accounting and ATM RMON
Signaling diagnostics and MIB	*ATM Switch Router Software Configuration Guide*: • Configuring Signalling Features • Configuring Signalling Diagnostics Tables
SNMP[2] (v1, v2, and v3)	*Cisco IOS Configuration Fundamentals Configuration Guide*, *Release 12.2*: • System Management • Configuring SNMP Support
Web Console	*Cisco 6400 Software Setup Guide*: • Web Console

1. RMON = remote monitoring
2. SNMP = Simple Network Management Protocol

QoS

Table 1-22 NSP Features—QoS

Feature	Documentation
ATM Policing by Service Category for SVC/SoftPVC	*ATM Policing by Service Category for SVC/SoftPVC*, 12.2(4)B feature module

RADIUS/AAA

Table 1-23 NSP Features—RADIUS/AAA

Feature	Documentation
TACACS+ (admin login only)	*ATM Switch Router Software Configuration Guide*: • Configuring System Management Functions • Configuring TACACS *Cisco IOS Security Configuration Guide, Release 12.2*: • Security Server Protocols • Configuring TACACS+

Scalability and Performance

Table 1-24 NSP Features—Scalability and Performance

Feature	Documentation
Capability to view used/unused ITT[1] blocks	*Cisco 6400 Software Setup Guide*: • Optimizing the Number of Virtual Connections on the Cisco 6400 • Displaying ITT Allocation
Fragmentation minimization	*Cisco 6400 Software Setup Guide*: • Optimizing the Number of Virtual Connections on the Cisco 6400
ITT block shrinking	*Cisco 6400 Software Setup Guide*: • Optimizing the Number of Virtual Connections on the Cisco 6400

1. ITT = Input Translation Table

Signaling and Routing

Table 1-25 NSP Features—Signaling and Routing

Feature	Documentation
ATM NSAP[1] and left-justified E.164 address support	*ATM Switch Router Software Configuration Guide*: • Configuring Signalling Features • Configuring E.164 Addresses *ATM and Layer 3 Switch Router Command Reference*: • A Commands • aesa embedded-number left-justified
CUG[2] for ATM VPNs	*ATM Switch Router Software Configuration Guide*: • Configuring Signalling Features • Configuring Closed User Group Signalling
E.164 address translation and autoconversion	*ATM Switch Router Software Configuration Guide*: • Configuring Signalling Features • Configuring E.164 Addresses
Hierarchical PNNI[3]	*ATM Switch Router Software Configuration Guide*: • Configuring ATM Routing and PNNI • Basic PNNI Configuration *Guide to ATM Technology*: • ATM Routing with IISP and PNNI • PNNI Overview • Hierarchical PNNI
ILMI[4] 4.0	*ATM Switch Router Software Configuration Guide* • Configuring ILMI
IISP[5]	*Cisco 6400 Software Setup Guide*: • Node Line Card Interface Configuration • ATM Interface Types • Interim Interswitch Signaling Protocol Interfaces *Guide to ATM Technology*: • ATM Routing with IISP and PNNI • Static Routing with IISP

Table 1-25 NSP Features—Signaling and Routing (continued)

Feature	Documentation
UNI[6] 3.0, UNI 3.1, and UNI 4.0	*Cisco 6400 Software Setup Guide*: • Node Line Card Interface Configuration • ATM Interface Types • User-Network Interfaces
VPI/VCI range support in ILMI 4.0	*ATM Switch Router Software Configuration Guide*: • Configuring Virtual Connections • Configuring a VPI/VCI Range for SVPs and SVCs

1. NSAP = network service access point
2. CUG = closed user group
3. PNNI = Private Network-Network Interface
4. ILMI = Interim Local Management Interface
5. IISP = Interim-Interswitch Signaling Protocol
6. UNI = User-Network Interface

CHAPTER 2

Layer 2 Tunnel Protocol

This chapter provides tasks and restrictions for Layer 2 tunnel protocol (L2TP) features supported by the Cisco 6400 in Cisco IOS Release 12.2(4)B.

This chapter only describes tasks that are specific to the Cisco 6400 and supplements the following documentation:

Documentation	Relevant Information
"Session and Tunnel Scalability" chapter	Describes parameters used to optimize the session and tunnel scalability on the Cisco 6400.
"Supported Features" chapter	Includes a complete list of L2TP and L2TP-related features supported in Cisco IOS Release 12.2(4)B.
Cisco IOS Dial Technologies Configuration Guide	Provides general L2TP overview, configuration, verification, monitoring, and troubleshooting information.
Layer 2 Tunnel Protocol feature module	Provides general L2TP overview, configuration, verification, monitoring, and troubleshooting information.

This chapter includes the following sections:

See the "Supported Features" chapter for additional documentation on L2TP features.

Restrictions

L2TP Tunnel Service Authorization Feature Restriction

Static tunnel service authorization does not support switched virtual channels (SVCs).

L2TP Tunnel Switching Feature Restriction

When using a RADIUS service profile for tunnel service authorization, the NRP configured as an L2TP tunnel switch must forward all sessions through L2TP tunnels. The L2TP tunnel switch must not terminate any of the sessions.

L2TP Multihop Feature Restriction

L2TP Multihop by remote tunnel hostname is not supported in Cisco IOS Release 12.2(4)B3.

L2TP Multihop by domain is supported in Cisco IOS Release 12.2(4)B3 with the following required configuration:

Enter the **lcp renegotiation always** configuration command on the L2TP network server (LNS) vpdn-group.

Basic LAC Configuration

The L2TP access concentrator (LAC) acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP network server (LNS). The LAC sits between an LNS and a remote system and forwards packets to and from each. Packets sent from the LAC to the LNS require tunneling with the L2TP protocol, and the connection from the LAC to the remote system is either local or a PPP link.

Configuring the LAC

Enter the following commands to enable VPDN on a LAC by using L2TP beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vpdn enable`	Enables VPDN and informs the router to look for tunnel definitions from an LNS.
Step 2	`Router(config)# vpdn group group-number`	Defines a local group number identifier for which other VPDN variables can be assigned. Valid group numbers range between 1 and 3000.
Step 3	`Router(config-vpdn)# request-dialin l2tp ip ip-address {domain domain-name | dnis dialed-number}`	Enables the router to request a dial-in tunnel to an IP address if the dial-in user belongs to a specific domain or the dial-in user dialed a specific DNIS.

Basic LNS Configuration

The L2TP network server (LNS) is the termination point for an L2TP tunnel and is a peer to the LAC. The LNS is the logical termination point of a PPP session that is being tunneled from the remote system by the LAC. Basic LNS configuration consists of the following tasks:

- Task 1: Configuring the LNS to Initiate and Receive Calls
- Task 2: Configuring the Virtual Template Interface

You can configure the virtual template interface with configuration parameters you want to apply to virtual access interfaces. A virtual template interface is a logical entity configured for a serial interface, is not tied to any physical interface, and is applied dynamically as needed. Virtual access interfaces are *cloned* from a virtual template interface, used on demand, and then freed when no longer needed.

Task 1: Configuring the LNS to Initiate and Receive Calls

To configure the LNS to initiate and receive calls, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vpdn enable`	Enables VPDN and informs the router to look for tunnel definitions from an LNS.
Step 2	`Router(config)# vpdn group` *group-number*	Defines a local group number identifier for which other VPDN variables can be assigned. Valid group numbers range between 1 and 3000.
Step 3	`Router(config-vpdn)# accept dialin l2tp virtual-template` *virtual-template-number* `remote` *remote-peer-name*	Allows the LNS to accept an open tunnel request from the specified remote peer and identify the virtual template to use for cloning virtual access interfaces.

Task 2: Configuring the Virtual Template Interface

To create and configure a virtual template interface, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface virtual-template` *number*	Creates a virtual template interface and enters interface configuration mode.
Step 2	`Router(config-if)# ip unnumbered ethernet 0`	Enables IP without assigning a specific IP address on the LAN.
Step 3	`Router(config-if)# encapsulation ppp`	Enables PPP encapsulation on the virtual template interface, which will be applied to virtual access interfaces.
Step 4	`Router(config-if)# ppp authentication {pap | chap}`	Enables PAP or CHAP authentication on the virtual template interface, which will be applied to virtual access interfaces.

Optionally, you can configure other commands for the virtual template interface. For information about configuring virtual template interfaces, see the "Configuring Virtual Template Interfaces" chapter in the "Virtual Templates, Profiles, and Networks" part of the *Cisco IOS Dial Technologies Configuration Guide*.

Tunnel Service Authorization Enhancements

Note Before configuring this feature, see the "Restrictions" section on page 2-2.

The tunnel service authorization enhancements enable the LAC to conduct static or dynamic tunnel service authorization. A static domain name can be configured on the ATM PVC port (directly or through a VC class) to override the domain name supplied by the client. If a static domain name is not configured, the LAC conducts dynamic tunnel service authorization, which includes two steps.

1. Domain Preauthorization—The LAC checks the client-supplied domain name against an authorized list configured on the RADIUS server for each PVC. If successful, the LAC proceeds to tunnel service authorization. If domain preauthorization fails, the LAC attempts PPP authentication/authorization for local termination.
2. Tunnel Service Authorization—The user profile on the RADIUS server provides a list of domains accessible to the user, enabling tunnel service authorization for the client-supplied domain. If successful, the LAC establishes an L2TP tunnel.

The tunnel service authorization enhancements provide the following benefits:

- Selecting tunnels by virtual connection—Static tunnel service authorization enables all PPP sessions originating from a particular PVC to be sent to the same L2TP tunnel.
- Supporting unstructured usernames—By configuring static domain names, usernames without domain names can undergo tunnel service authorization.
- Preventing arbitrary tunnel creation—Domain preauthorization prevents users from creating tunnels to arbitrary LNSes by simply reconfiguring the domains on the client equipment.

To configure the tunnel service authorization enhancements, complete the following tasks:

- Task 1 (Option 1): Configuring a Static Domain Name (PVC Method)
- Task 1 (Option 2): Configuring a Static Domain Name (VC Class Method)
- Task 2: Enabling Domain Preauthorization
- Task 3: Configuring Communication with the RADIUS Server
- Task 4: Configuring the RADIUS User Profile for Domain Preauthorization
- Task 5: Configuring the RADIUS Service Profile for Tunnel Service Authorization

Task 1 (Option 1): Configuring a Static Domain Name (PVC Method)

To configure the static domain name directly on the PVC, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface atm 0/0/0[.subinterface-number] {multipoint | point-to-point | tag-switching}`	Specifies the ATM interface and optional subinterface.
Step 2	`Router(config-subif)# no ip directed-broadcast`	Disables forwarding of directed broadcasts.
Step 3	`Router(config-subif)# pvc [name] vpi/vci`	Configures a PVC on the ATM interface or subinterface.

	Command	Purpose
Step 4	`Router(config-if-atm-vc)# encapsulation aal5mux ppp Virtual-Template` *number*	Sets encapsulation as PPP. Also specifies the virtual template interface to clone for the new virtual access interface.
Step 5	`Router(config-if-atm-vc))# vpn service` *domain-name*	Configures the static domain name on the PVC.

Example: Configuring a Static Domain Name (PVC Method)

The following example shows the static domain names “net1.com” and “net2.com” assigned to PVCs on an ATM interface. All PPP sessions originating from PVC 30/33 are sent to the “net1.com” L2TP tunnel; all PPP sessions originating from PVC 30/34 are sent to the “net2.com” tunnel.

```
!
interface ATM 0/0/0.33 multipoint
  pvc 30/33
   encapsulation aal5ciscoppp Virtual-Template1
   vpn service net1.com
  !
  pvc 30/34
   encapsulation aal5ciscoppp Virtual-Template1
   vpn service net2.com
  !
```

Task 1 (Option 2): Configuring a Static Domain Name (VC Class Method)

To configure the static domain name on the VC class, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vc-class atm` *vc-class-name*	Creates and names a map class.
Step 2	`Router(config-vc-class)# encapsulation aal5mux ppp Virtual-Template` *number*	Sets encapsulation as PPP. Also specifies the virtual template interface to clone for the new virtual access interface.
Step 3	`Router(config-vc-class)# vpn service` *domain-name*	Configures the static domain name on the VC class.
Step 4	`Router(config-vc-class)# exit`	Returns to global configuration mode.
Step 5	`Router(config)# interface atm 0/0/0`[*.subinterface-number*] {**multipoint** | **point-to-point** | **tag-switching**}	Specifies the ATM interface and optional subinterface.
Step 6	`Router(config-subif)# class-int` *vc-class-name*	Applies the VC class to all VCs on the ATM interface or subinterface.

Example: Configuring a Static Domain Name (VC Class Method)

In the following example, the static domain name "net.com" is assigned to a VC class. The VC class is then assigned to the VCs on an ATM subinterface.

```
!
vc-class ATM MyClass
  encapsulation aal5ciscoppp Virtual-Template1
  vpn service net.com
  !
interface ATM 0/0/0.99 multipoint
  class-int MyClass
  no ip directed-broadcast
  pvc 20/40
  pvc 30/33
  !
```

Verifying the Static Domain Name

To verify that you successfully configured the static domain name, enter the **show running-config** EXEC command.

Task 2: Enabling Domain Preauthorization

To enable the LAC to perform domain authorization before tunneling, enter the following command in global configuration mode:

Command	Purpose
`Router(config)# vpdn authorize domain`	Enables domain preauthorization.

Dynamic tunnel service authorization requires additional commands for proper communication with the RADIUS server. See the "Task 3: Configuring Communication with the RADIUS Server" section.

Example: Enabling Domain Preauthorization

The following example shows the configuration necessary for the LAC to participate in domain preauthorization:

```
!
aaa new-model
aaa authorization network default local group radius
!
➔ vpdn authorize domain
!
radius-server host 10.9.9.9 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
radius-server key MyKey
radius-server vsa send authentication
!
```

Verifying Domain Preauthorization

To check that you successfully enabled domain preauthorization, enter the **show running-config** EXEC command.

Task 3: Configuring Communication with the RADIUS Server

To enable the LAC to communicate properly with the RADIUS server for tunnel service authorization, complete following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number]`	Specifies the RADIUS server host.
Step 2	`Router(config)# radius-server attribute nas-port format d`	Selects the ATM VC extended NAS port format for RADIUS accounting features.
Step 3	`Router(config)# radius-server key string`	Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
Step 4	`Router(config)# radius-server vsa send authentication`	Configures the LAC to recognize and use vendor-specific attributes.

Example: Configuring Communication with the RADIUS Server

The following example shows the configuration necessary for the LAC to participate in tunnel service authorization:

```
!
aaa new-model
aaa authorization network default local group radius
!
radius-server host 10.9.9.9 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
radius-server key MyKey
radius-server vsa send authentication
!
```

Verifying the Communication with the RADIUS Server Configuration

To check that you successfully configured the LAC to communicate properly with the RADIUS server for tunnel service authorization, enter the **show running-config** EXEC command.

Task 4: Configuring the RADIUS User Profile for Domain Preauthorization

To enable domain preauthorization, enter the following configuration in the user profile on the RADIUS server:

RADIUS Entry	Purpose
nas-port:*ip-address:slot/subslot/port/vpi.vci*	Configures the NAS port username for domain preauthorization. Includes the management IP address of the NSP.
Password = "cisco"	Sets the fixed password.
User-Service-Type = Outbound-User	Configures the service-type as outbound.
Cisco-AVpair = "vpdn:vpn-domain-list=*domain1, domain2,...***"**	Specifies the domains accessible to the user.

Example: Configuring the RADIUS User Profile for Domain Preauthorization

The following example shows a domain preauthorization RADIUS user profile:

```
user = nas-port:10.9.9.9:0/0/0/30.33{
 profile_id = 826
 profile_cycle = 1
 radius=Cisco {
 check_items= {
 2=cisco
 }
 reply_attributes= {
 9,1="vpdn:vpn-domain-list=net1.com,net2.com"
 6=5
 }
 }

 }
```

Verifying the RADIUS User Profile for Domain Preauthorization

To verify the RADIUS user profile, refer to the user documentation for your RADIUS server.

Task 5: Configuring the RADIUS Service Profile for Tunnel Service Authorization

To enable tunnel service authorization, use the following configuration in the service profile on the RADIUS server:

RADIUS Entry	Purpose
domain **Password "cisco"**	Sets the fixed password for the client-supplied domain.
User-Service-Type = Outbound-User	Configures the service-type as outbound.
Cisco-AVpair = "vpdn:tunnel-id=*name***"**	Specifies the name of the tunnel that must match the LNS's VPDN terminate-from hostname.

RADIUS Entry	Purpose
Cisco-AVpair = "vpdn:l2tp-tunnel-password=*secret***"**	Specifies the secret password for L2TP tunnel authentication.
Cisco-AVpair = "vpdn:tunnel-type=l2tp"	Specifies the Layer 2 Tunnel Protocol.
Cisco-AVpair = "vpdn:ip-addresses=*ip-address***"**	Specifies the IP address of LNS.

Example: Configuring the RADIUS Service Profile for Tunnel Service Authorization

The following example shows a tunnel service authorization RADIUS service profile:

```
user = net1.com{
profile_id = 45
profile_cycle = 18
member = me
radius=Cisco {
check_items= {
2=cisco
}
reply_attributes= {
9,1="vpdn:tunnel-id=LAC-1"
9,1="vpdn:l2tp-tunnel_password=MySecret"
9,1="vpdn:tunnel-type=l2tp"
9,1="vpdn:ip-addresses=10.10.10.10"
6=5
}
}
}
```

Verifying the RADIUS Service Profile for Tunnel Service Authorization

To verify the RADIUS service profile, refer to the user documentation for your RADIUS server.

Sessions per Tunnel Limiting

This feature enables the **initiate-to** command to limit the number of sessions per L2TP tunnel. Choose one method to configure this feature:

- Option 1: Configuring Sessions Per Tunnel Limiting on the LAC
- Option 2: Configuring Sessions per Tunnel Limiting in the RADIUS Service Profile

Option 1: Configuring Sessions Per Tunnel Limiting on the LAC

To limit the number of sessions per tunnel without using a RADIUS server, complete the following steps on the NRP-LAC beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)#` **vpdn-group** *number*	Selects the VPDN group.
Step 2	`Router(config-vpdn)#` **request-dialin**	Enables the LAC to request L2TP tunnels to the LNS. Enters VPDN request-dialin group mode.

	Command	Purpose
Step 3	`Router(config-vpdn-req-in)# protocol l2tp`	Specifies the Layer 2 Tunnel Protocol.

Step 4	`Router(config-vpdn-req-in)# multihop hostname ingress-tunnel-name`
	or
	`Router(config-vpdn-req-in)# domain domain-name`
	or
	`Router(config-vpdn-req-in)# dnis dnis-number`
		Initiates a tunnel based on the LAC's host name or ingress tunnel ID.
		Initiates a tunnel based on the client-supplied domain name.
		Initiates a tunnel based on the user's DNIS number.

Step 5	`Router(config-vpdn-req-in)# exit`	Returns to VPDN group mode.
Step 6	`Router(config-vpdn)# initiate-to ip ip-address limit limit-number [priority priority-number]`	Specifies the LNS IP address and the maximum number of sessions per tunnel. Optionally specifies the priority of the IP address (1 is highest).

Example: Configuring Sessions Per Tunnel Limiting on the LAC

In the following example, the LAC initiates up to three tunnels. Each tunnel is limited to 40 sessions.

```
!
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
!
```

Verifying Sessions per Tunnel Limiting on the LAC

Step 1 Enter the **show running-config** EXEC command to check that you successfully configured the maximum number of sessions per tunnel.

Step 2 Enter the **show vpdn tunnel** privileged EXEC command to verify that the number of displayed sessions does not exceed your configured limit.

```
Router# show vpdn tunnel

L2TP Tunnel Information (Total tunnels 50 sessions 2000)

LocID RemID Remote Name   State  Remote Address  Port Sessions
41234 7811  LNS1          est    10.1.1.1        1701 40
20022 2323  LNS1          est    10.1.1.1        1701 40
41234 7811  LNS2          est    10.1.2.2        1701 40
59765 3477  LNS2          est    10.1.3.3        1701 40
...
```

Option 2: Configuring Sessions per Tunnel Limiting in the RADIUS Service Profile

To use a RADIUS server to limit the number of sessions per tunnel, enter the following Cisco-AVpair attributes in the RADIUS service profile:

- VPDN IP Addresses
- VPDN IP Address Limits

VPDN IP Addresses

This attribute specifies the IP addresses of the LNSs to receive the L2TP connections.

Cisco-AVpair = "vpdn:ip-addresses=*address1*[<*delimiter*>*address2*][<*delimiter*>*address3*]..."

Syntax Description

address		IP address of the LNS.
<*delimiter*>	, (comma)	Selects load sharing among IP addresses.
	(space)	Selects load sharing among IP addresses.
	/ (slash)	Groups IP addresses on left side in higher priority than the right side.

In the following example, the LAC sends the first PPP session through a tunnel to 10.1.1.1, the second PPP session to 10.2.2.2, and the third to 10.3.3.3. The fourth PPP session is sent through the tunnel to 10.1.1.1, and so forth. If the LAC fails to establish a tunnel with any of the IP addresses in the first group, then the LAC attempts to connect to those in the second group (10.4.4.4 and 10.5.5.5).

Example (RADIUS Freeware Format)

```
Cisco-AVpair="vpdn:ip-addresses=10.1.1.1,10.2.2.2,10.3.3.3/10.4.4.4,10.5.5.5"
```

Example (CiscoSecure ACS for UNIX)

```
9,1="vpdn:ip-addresses=10.1.1.1,10.2.2.2,10.3.3.3/10.4.4.4,10.5.5.5"
```

VPDN IP Address Limits

This attribute specifies the maximum number of sessions in each tunnel to the IP addresses listed with the **vpdn:ip-addresses** attribute.

Cisco-AVpair = "vpdn:ip-address-limits=*limit1* [*limit2*] [*limit3*]... "

Syntax Description

limit	Maximum number of sessions per tunnel to the corresponding IP address.

Example (RADIUS Freeware Format)

```
Cisco-AVpair="vpdn:ip-address-limits=10 20 30 40 50 "
```

Example (CiscoSecure ACS for UNIX)

```
9,1="vpdn:ip-address-limits=10 20 30 40 50 "
```

Note You must enter a space between the final *limit* entry and the end quotation marks.

Example: Configuring Sessions per Tunnel Limiting in the RADIUS Service Profile

The following example shows a tunnel service authorization RADIUS service profile with the session limiting entry. IP addresses 10.1.1.1 and 10.2.2.2 are assigned priority 1; IP addresses 10.3.3.3 and 10.4.4.4 are assigned priority 2. Tunnels to 10.1.1.1 are limited to 100 sessions, tunnels to 10.2.2.2 are limited to 200 sessions, tunnels to 10.3.3.3 are limited to 300 sessions, and tunnels to 10.4.4.4 are limited to 400 sessions.

```
user = net.com{
profile_id = 45
profile_cycle = 18
member = me
radius=Cisco {
check_items= {
2=cisco
}
reply_attributes= {
9,1="vpdn:tunnel-id=LAC-1"
9,1="vpdn:l2tp-tunnel_password=MySecret"
9,1="vpdn:tunnel-type=l2tp"
9,1="vpdn:ip-addresses=10.1.1.1 10.2.2.2/10.3.3.3 10.4.4.4"
9,1="vpdn:ip-address-limits=100 200 300 400 "
6=5
}
}
}
```

Verifying Sessions per Tunnel Limiting in the RADIUS Service Profile

To verify the RADIUS service profile, refer to the user documentation for your RADIUS server.

Tunnel Sharing

This feature enables sessions that are authorized with different domains to share the same tunnel. Tunnel sharing reduces the number of tunnels required from the LAC. When used with the L2TP Tunnel Switching feature, tunnel sharing also reduces the number of tunnels to an LNS. While improving tunnel management, tunnel sharing helps to reduce the number of tunnel establishment messages that are sent after interface dropouts, reducing dropout recovery time.

Tunnel Sharing configuration consists of the following tasks:

- Task 1: Configuring Tunnel Sharing on the LAC
- Task 2: Configuring Tunnel Sharing in the RADIUS Service Profile

Task 1: Configuring Tunnel Sharing on the LAC

To implement the tunnel sharing feature, complete the following steps on the NRP-LAC beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vpdn-group number`	Selects the VPDN group.
Step 2	`Router(config-vpdn)# request-dialin`	Enables the LAC to request L2TP tunnels to the LNS. Enters VPDN request-dialin group mode.
Step 3	`Router(config-vpdn-req-in)# protocol l2tp`	Specifies the Layer 2 Tunnel Protocol.

Step 4	`Router(config-vpdn-req-in)# multihop hostname ingress-tunnel-name`
	or
	`Router(config-vpdn-req-in)# domain domain-name`
	or
	`Router(config-vpdn-req-in)# dnis dnis-number`
	(Repeat this step to enter all keys chosen for tunnel sharing)
		Initiates a tunnel based on the LAC's host name or ingress tunnel ID.
		Initiates a tunnel based on the client-supplied domain name.
		Initiates a tunnel based on the user's DNIS number.

Step 5	`Router(config-vpdn-req-in)# exit`	Returns to the VPDN group mode.
Step 6	`Router(config-vpdn)# initiate-to ip ip-address [priority priority-number]`	Specifies the LNS IP address. Optionally specifies the priority of the IP address (1 is highest).
Step 7	`Router(config-vpdn)# tunnel share`	Enables tunnel sharing among the keys entered in Step 4.

Example: Configuring Tunnel Sharing on the LAC

In the following example, all sessions that are locally authorized through VPDN group 1 are 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
!
```

Verifying Tunnel Sharing Configuration on the LAC

Enter the **show running-config** EXEC command to check that you successfully enabled the tunnel sharing feature.

Task 2: Configuring Tunnel Sharing in the RADIUS Service Profile

To implement the tunnel sharing feature, enter the following Cisco-AVpair attributes in the RADIUS service profile:

- VPDN Group
- Tunnel Share

VPDN Group

This attribute specifies the group to which the service belongs. All services with matching group names are considered members of the same VPDN group.

Cisco-AVpair = "vpdn:vpdn-group=*group-name***"**

Example (RADIUS Freeware Format)

```
Cisco-AVpair="vpdn:vpdn-group=group1"
```

Example (CiscoSecure ACS for UNIX)

```
9,1="vpdn:vpdn-group=group1"
```

Tunnel Share

This attribute indicates that the tunnel sharing feature is enabled for the service.

Cisco-AVpair = "vpdn:tunnel-share=yes"

Syntax Description

This attribute has no arguments or keywords.

Example (RADIUS Freeware Format)

```
Cisco-AVpair="vpdn:tunnel-share=yes"
```

Example (CiscoSecure ACS for UNIX)

```
9,1="vpdn:tunnel-share=yes"
```

Example: Configuring Tunnel Sharing in the RADIUS Service Profile

In the following example, both the net1.com and net2.com services are members of the “group1” VPDN group. With tunnel sharing enabled in both service profiles, the sessions for net1.com and net2.com will be combined and sent through the same tunnels.

```
user = net1.com{
profile_id = 45
profile_cycle = 18
member = me
radius=Cisco {
check_items= {
2=cisco
}
reply_attributes= {
9,1="vpdn:tunnel-id=LAC-1"
9,1="vpdn:l2tp-tunnel_password=MySecret"
```

```
9,1="vpdn:tunnel-type=l2tp"
9,1="vpdn:ip-addresses=10.10.10.10"
9,1="vpdn:vpdn-group=group1"
9,1="vpdn:tunnel-share=yes"
6=5
}
}
}

user = net2.com{
profile_id = 45
profile_cycle = 18
member = me
radius=Cisco {
check_items= {
2=cisco
}
reply_attributes= {
9,1="vpdn:tunnel-id=LAC-1"
9,1="vpdn:l2tp-tunnel_password=MySecret"
9,1="vpdn:tunnel-type=l2tp"
9,1="vpdn:ip-addresses=10.10.10.10"
9,1="vpdn:vpdn-group=group1"
9,1="vpdn:tunnel-share=yes"
6=5
}
}
}
```

Verifying the Tunnel Sharing Configuration in the RADIUS Service Profile

To verify the RADIUS service profile, refer to the user documentation for your RADIUS server.

Tunnel Switching

Note Before configuring this feature, read the "Restrictions" section on page 2-2.

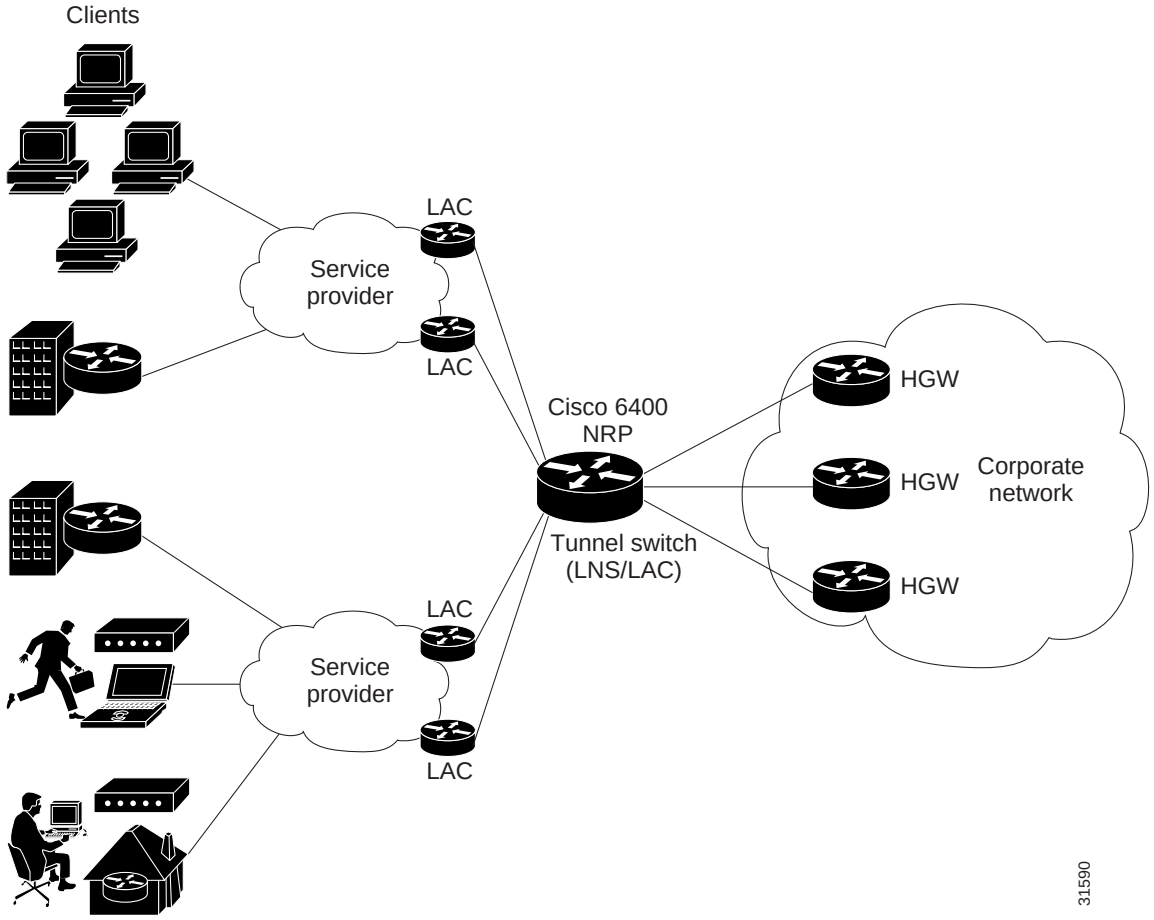
The L2TP Tunnel Switching feature enables the NRP to terminate tunnels from LACs and forward the sessions through new L2TP tunnels selected independently of the client-supplied domains. The NRP as a tunnel switch performs VPDN tunnel authorization based on the ingress tunnel names that are mapped to specified LNSs.

Tunnel switching provides the following benefits:

- Improved Provisioning Scalability—Aggregating LAC tunnels with an L2TP tunnel switch improves provisioning scalability on both the LAC and wholesaler ends.
- Improved Permanent Virtual Circuit Interconnect Scalability—In a B-ISDN network, a multihop node can improve PVC interconnect scalability.

Figure 2-1 shows an example network topology using the L2TP Tunnel Switching feature.

Figure 2-1 Example Network Topology Using the L2TP Tunnel Switching Feature



To configure the L2TP Tunnel Switching feature, complete the following tasks:

- Task 1: Enabling VPDN and Multihop Functionality
- Task 2: Terminating the Tunnel from the LAC
- Task 3: Mapping the Ingress Tunnel Name to an LNS
- Task 4: Performing VPDN Tunnel Authorization Searches by Ingress Tunnel Name

Note The NRP as a tunnel switch requires at least two VPDN groups: one to handle incoming tunnels from the LAC, and one to create the L2TP tunnels/sessions to the LNS.

Task 1: Enabling VPDN and Multihop Functionality

To use the L2TP Tunnel Switching feature, you must first enable VPDN and multihop capabilities by entering the following commands in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vpdn enable`	Enables VPDN functionality.
Step 2	`Router(config)# vpdn multihop`	Enables VPDN multihop functionality.

Verifying VPDN and Multihop Functionality

To verify that you enabled VPDN and multihop functionality, enter the **show running-config** EXEC command.

Task 2: Terminating the Tunnel from the LAC

To terminate the tunnel from the LAC, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# username` *remote-hostname* `password` *secret*	Configures the secret password. Must match the secret password configured on the LAC.
Step 2	`Router(config)# username` *local-name* `password` *secret*	Configures the secret password. Must match *secret* in Step 1.
Step 3	`Router(config)# vpdn-group` *number*	Selects the VPDN group.
Step 4	`Router(config-vpdn)# accept-dialin`	Accepts incoming L2TP tunnel connections. Enters VPDN accept-dialin group mode.
Step 5	`Router(config-vpdn-acc-in)# protocol l2tp`	Specifies the Layer 2 Tunnel Protocol.
Step 6	`Router(config-vpdn-acc-in)# virtual-template` *number*	Specifies the virtual template interface to clone the new virtual access interface.
Step 7	`Router(config-vpdn-acc-in)# exit`	Returns to the VPDN group mode.
Step 8	`Router(config-vpdn)# terminate-from hostname` *remote-hostname*	Specifies the host name of the remote LAC that will be required when accepting a VPDN tunnel. Must match *remote-hostname* in Step 1.
Step 9	`Router(config)# lcp renegotiation always`	Allows the LNS to renegotiate the LCP on dial-in calls.
Step 10	`Router(config-vpdn)# local name` *local-name*	Specifies the local host name of the tunnel. Must match *local-name* in Step 2.

Verifying Termination of the Tunnel from the LAC

To verify that you successfully configured the tunnel switch to terminate tunnels from the LAC, enter the **show running-config** EXEC command.

Task 3: Mapping the Ingress Tunnel Name to an LNS

To map the ingress tunnel name to an LNS, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# username username password secret`	Configures the secret password. Username must match LNS's hostname or tunnel ID. Secret password must match the secret configured on the LNS.
Step 2	`Router(config)# username egress-tunnel-name password secret`	Configures the secret password. Must match *secret* in Step 1.
Step 3	`Router(config)# vpdn-group number`	Selects the VPDN group.
Step 4	`Router(config-vpdn)# request-dialin`	Enables the tunnel switch to request L2TP tunnels to the LNS. Enters VPDN request-dialin group mode.
Step 5	`Router(config-vpdn-req-in)# protocol l2tp`	Specifies the Layer 2 Tunnel Protocol.
Step 6	`Router(config-vpdn-req-in)# multihop hostname ingress-tunnel-name`	Initiates a tunnel based on the LAC's hostname or ingress tunnel ID.
Step 7	`Router(config-vpdn-req-in)# exit`	Returns to the VPDN group mode.
Step 8	`Router(config-vpdn)# initiate-to ip ip-address [limit limit-number] [priority priority-number]`	Specifies the LNS. Optionally specifies the maximum number of sessions per tunnel as well as the priority of the IP address (1 is highest).
Step 9	`Router(config-vpdn)# local name egress-tunnel-name`	Specifies the local host name of the tunnel. Must match *egress-tunnel-name* in Step 2.

Verifying the Ingress Tunnel Name to LNS Map

To verify that you successfully mapped the ingress tunnel name to the LNS, enter the **show running-config** EXEC command.

Task 4: Performing VPDN Tunnel Authorization Searches by Ingress Tunnel Name

To specify how to perform VPDN tunnel authorization searches, enter the following command in global configuration mode:

Command	Purpose
`Router(config)# vpdn search-order {multihop-hostname dnis domain}`	Specifies a search order. You can specify to search by onfigured ingress tunnel name (multihop-hostname), domain, and/or DNIS. The order you specify in the command controls the order of the resulting search.

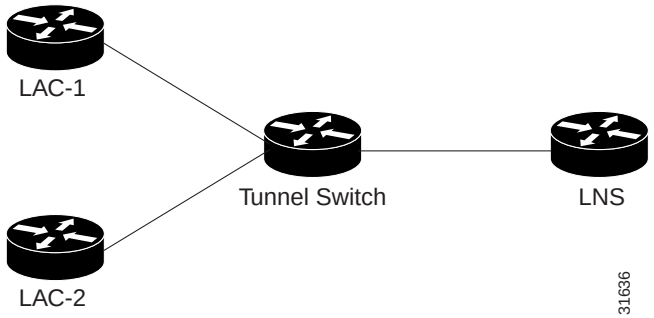
Verifying VPDN Tunnel Authorization Searches by Ingress Tunnel Name

To verify that you successfully configured the tunnel switch to perform VPDN tunnel authorization searches by ingress tunnel name, enter the **show running-config** EXEC command.

Comprehensive Example: L2TP Tunnel Switching Configurations

The examples in this section show the configurations necessary for the basic L2TP tunnel switch topology shown in Figure 2-2. In this topology, a tunnel switch terminates tunnels from two LACs and forwards all the sessions through one tunnel to the LNS.

Figure 2-2 Example L2TP Tunnel Switch Topology



This section provides the following configuration examples:

- Example: LAC-1 Configuration
- Example: LAC-2 Configuration
- Example: L2TP Tunnel Switch Configuration
- Example: LNS Configuration

Example: LAC-1 Configuration

In the following example, LAC-1 performs tunnel authorization based on domain name and initiates a tunnel to the L2TP tunnel switch:

```
!
vpdn enable
!
username net.com password Secret1
username Tunnel-Switch-In password Secret1
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain service1.net.com
 initiate-to ip 10.1.1.1
 local name net.com
!
```

Example: LAC-2 Configuration

In the following example, LAC-2 also performs tunnel authorization based on domain name and initiates a tunnel to the L2TP tunnel switch:

```
!
vpdn enable
!
username net.com password Secret2
username Tunnel-Switch-In password Secret2
!
vpdn-group 1
 request-dialin
  protocol l2tp
  domain service2.net.com
 initiate-to ip 10.1.1.1
 local name net.com
!
```

Example: L2TP Tunnel Switch Configuration

In the following example, the NRP is configured as an L2TP tunnel switch. VPDN groups 1 and 2 are used to terminate the tunnels from the LAC. VPDN group 11 is used to initiate the tunnel to the LNS, and it performs tunnel authorization based on the configured ingress tunnel name.

```
!
vpdn enable
vpdn multihop
vpdn search-order multihop-hostname domain
!
username net.com password Secret1
username Tunnel-Switch-In password Secret1
username net.com password Secret2
username Tunnel-Switch-In password Secret2
username LNS password Secret3
username Tunnel-Switch-Out password Secret3
!
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname net.com
```

```
 local name Tunnel-Switch-In
!
vpdn-group 11
 request-dialin
  protocol l2tp
  multihop hostname net.com
 initiate-to ip 10.2.2.2
 local name Tunnel-Switch-Out
!
interface ATM 0/0/0.1001 point-to-point
 ip address 10.1.1.1 255.255.255.0
 pvc 5/10
 encapsulation aal5snap
!
interface Virtual-Template 1
 ip unnumbered FastEthernet 0/0/0
 no ip directed-broadcast
 no keepalive
 no peer default ip address
 ppp authentication chap
!
```

Example: LNS Configuration

In the following example, the LNS terminates the tunnel from the L2TP tunnel switch:

```
vpdn enable
!
username LNS password Secret3
username Tunnel-Switch-Out password Secret3
!
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname Tunnel-Switch
 local name LNS
!
interface Virtual-Template 1
 ip unnumbered FastEthernet 0/0/0
 no ip directed-broadcast
 ip mroute-cache
 no keepalive
 peer default ip address pool pool-1
 ppp authentication chap
!
```

CHAPTER 3

Multiprotocol Label Switching

This chapter provides examples, restrictions, and prerequisites for multiprotocol label switching (MPLS) features supported by the Cisco 6400 in Cisco IOS Release 12.2(4)B.

This chapter only contains information that is specific to the Cisco 6400 and supplements the following documentation:

Documentation	Relevant Information
"Supported Features" chapter	Includes a complete list of MPLS and MPLS-related features supported in Cisco IOS Release 12.2(4)B.
Cisco IOS Switching Services Configuration Guide	Provides general MPLS overview, configuration, verification, monitoring, and troubleshooting information.
ATM Switch Router Software Configuration Guide	Provides general MPLS overview, configuration, verification, monitoring, and troubleshooting information. MPLS is called "Tag Switching" in this document.

This chapter includes the following sections:

Refer to the "Supported Features" chapter for documentation on additional MPLS features.

Restrictions

While configured as an MPLS Label Switch Controller (LSC), the NRP-2 or NRP-2SV can only support LSC functionality. The NRP-1 can also support network management on the Ethernet interface while configured as an MPLS LSC.

Prerequisites

In order to use the Cisco 6400 as an MPLS device, Cisco express forwarding (CEF) switching must be enabled on each NRP.

Split horizon is disabled by default on ATM interfaces. If you are running RIP in your MPLS VPNs, you must enable split horizon. See the "Split Horizon and RIP Example" section on page 3-16 for an example.

MPLS Edge Label Switch Router

The MPLS edge label switch router (Edge LSR) analyzes the Layer 3 header of a packet entering the MPLS network. The Edge LSR then maps the header information into a short fixed-length label and attaches the label to the packet. Inside the MPLS network, the ATM LSRs can forward these packets quickly by only looking at the label. When the packet exits the MPLS network, the Edge LSR removes the label and resumes Layer 3 forwarding of the packet.

Cisco 6400 NRPs can be configured as MPLS Edge LSRs that can be connected across MPLS networks by using permanent virtual paths (PVPs) or a virtual path identifier (VPI) range. The following sections provide simple examples of each scenario.

Note The Cisco 6400 NRP performs Edge LSR routing in compliance with RFC 1483 (aal5snap). Running any additional access protocols (such as PPP, RBE, or L2TP) on the same NRP is not supported.

The Edge LSR examples do not show the connections to the routers external to the MPLS network, but packets can enter and exit the MPLS network through the FastEthernet (FE) port on the Edge LSR NRP, or through a node line card (NLC) in the same Cisco 6400. The examples also do not show the devices within the MPLS or ATM network.

Note The recommended method of using an NSP to connect two MPLS Edge LSRs is to configure the NSP as a virtual path (VP) switch. A VP switch configuration is also recommended for an NSP connecting an MPLS Edge LSR to an ATM LSR. To configure the Cisco 6400 NSP as a VP switch, see the "Internal Cross-Connections" section of the "Basic NSP Configuration" chapter of the *Cisco 6400 Software Setup Guide*.

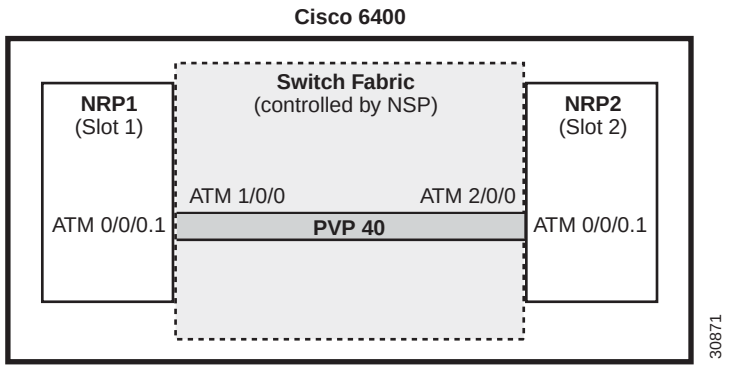
MPLS Edge LSRs Connected Through a PVP

The PVP configuration through the NSP provides transparent NSP redundancy. The NSP switchover does not preserve label virtual circuits (LVCs) unless they are aggregated into a PVP.

PVP Example: Configuring and Connecting Edge LSRs Within a Cisco 6400

In this example, two NRPs are configured as Edge LSRs in the same Cisco 6400. The Edge LSRs are connected to each other through a PVP through the switch fabric of the Cisco 6400, as shown in Figure 3-1.

Figure 3-1 PVP Connection Between Two Edge LSRs Within a Cisco 6400



The following example shows the configuration for NRP1 in Slot 1:

```
NRP1# configure terminal
NRP1(config)# ip cef
NRP1(config)# tag-switching ip
NRP1(config)# interface ATM0/0/0.1 tag-switching
NRP1(config-if)# ip unnumbered Loopback0
NRP1(config-if)# atm pvc 40 40 0 aal5snap
NRP1(config-if)# tag-switching atm vp-tunnel 40
NRP1(config-if)# tag-switching ip
```

The following example shows the configuration for NRP2 in Slot 2:

```
NRP2# configure terminal
NRP2(config)# ip cef
NRP2(config)# tag-switching ip
NRP2(config)# interface ATM0/0/0.1 tag-switching
NRP2(config-if)# ip unnumbered Loopback0
NRP2(config-if)# atm pvc 40 40 0 aal5snap
NRP2(config-if)# tag-switching atm vp-tunnel 40
NRP2(config-if)# tag-switching ip
```

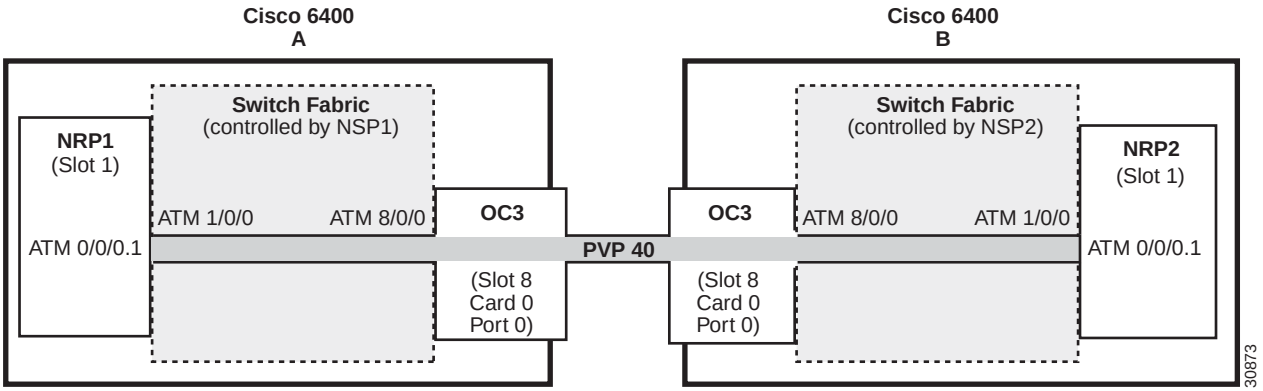
To complete the PVP connection between NRP1 and NRP2 in Figure 1, the NSP must be configured to set the path through the switch fabric. The following example shows the VP-switch configuration for the NSP:

```
NSP# configure terminal
NSP(config)# interface ATM1/0/0
NSP(config-if)# atm pvp 40  interface  ATM2/0/0 40
```

PVP Example: Configuring and Connecting Edge LSRs in Separate Cisco 6400s

In this example, two NRPs are configured as Edge LSRs in the separate Cisco 6400s. The Edge LSRs are connected to each other through a PVP through the MPLS network, as shown in Figure 3-2.

Figure 3-2 PVP Connection Between Two Edge LSRs in Separate Cisco 6400s



The following example shows the configuration for NRP1 in Slot 1 of Cisco 6400 A:

```
NRP1# configure terminal
NRP1(config)# ip cef
NRP1(config)# tag-switching ip
NRP1(config)# interface ATM0/0/0.1 tag-switching
NRP1(config-if)# ip unnumbered Loopback0
NRP1(config-if)# atm pvc 40 40 0 aal5snap
NRP1(config-if)# tag-switching atm vp-tunnel 40
NRP1(config-if)# tag-switching ip
```

The following example shows the configuration for NRP2 in Slot 1 of Cisco 6400 B:

```
NRP2# configure terminal
NRP2(config)# ip cef
NRP2(config)# tag-switching ip
NRP2(config)# interface ATM0/0/0.1 tag-switching
NRP2(config-if)# ip unnumbered Loopback0
NRP2(config-if)# atm pvc 40 40 0 aal5snap
NRP2(config-if)# tag-switching atm vp-tunnel 40
NRP2(config-if)# tag-switching ip
```

To complete the PVP connection between NRP1 and NRP2 in Figure 1, the NSPs must be configured to set the path through the switch fabric and node line cards (NLCs).

The following example shows the VP-switch configuration for NSP1 in Cisco 6400 A:

```
NSP1# configure terminal
NSP1(config)# interface ATM1/0/0
NSP1(config-if)# atm pvp 40  interface ATM8/0/0 40
```

The following example shows the VP-switch configuration for NSP2 in Cisco 6400 B:

```
NSP2# configure terminal
NSP2(config)# interface ATM1/0/0
NSP2(config-if)# atm pvp 40  interface ATM8/0/0 40
```

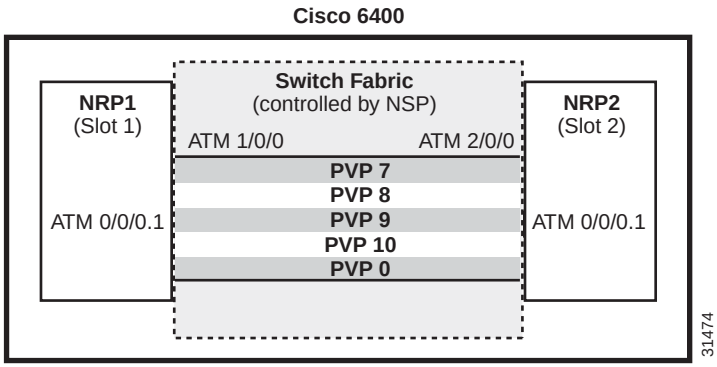
MPLS Edge LSRs Connected Through a VPI Range

In addition to providing transparent NSP redundancy, configuring a VPI Range to connect two MPLS Edge LSRs enables you to accommodate a large number of LVCs. For more information on VPI ranges, see the "Configuring a VPI Range" section in the "Configuring Tag Switching" chapter in the *ATM Switch Router Software Configuration Guide*.

VPI Range Example: Configuring and Connecting Edge LSRs Within a Cisco 6400

In this example, two NRPs are configured as Edge LSRs in the same Cisco 6400. The Edge LSRs are connected to each other through a VPI range through the switch fabric of the Cisco 6400, as shown in Figure 3-3.

Figure 3-3 VPI Range Between Two Edge LSRs Within a Cisco 6400



The following example shows the configuration for NRP1 in Slot 1:

```
NRP1# configure terminal
NRP1(config)# ip cef
NRP1(config)# tag-switching ip
NRP1(config)# interface ATM0/0/0.1 tag-switching
NRP1(config-if)# ip unnumbered Loopback0
NRP1(config-if)# tag-switching atm vpi 7-10
NRP1(config-if)# tag-switching ip
```

The following example shows the configuration for NRP2 in Slot 2:

```
NRP2# configure terminal
NRP2(config)# ip cef
NRP2(config)# tag-switching ip
NRP2(config)# interface ATM0/0/0.1 tag-switching
NRP2(config-if)# ip unnumbered Loopback0
NRP2(config-if)# tag-switching atm vpi 7-10
NRP2(config-if)# tag-switching ip
```

To complete the VPI range connection between NRP1 and NRP2 in Figure 1, the NSP must be configured to set the paths through the switch fabric. PVP 0 is used to set up the control channels. The following example shows the VP-switch configuration for the NSP:

```
NSP# configure terminal
NSP(config)# interface ATM1/0/0
NSP(config-if)# atm pvp 7 interface  ATM2/0/0 7
NSP(config-if)# atm pvp 8 interface  ATM2/0/0 8
NSP(config-if)# atm pvp 9 interface  ATM2/0/0 9
```

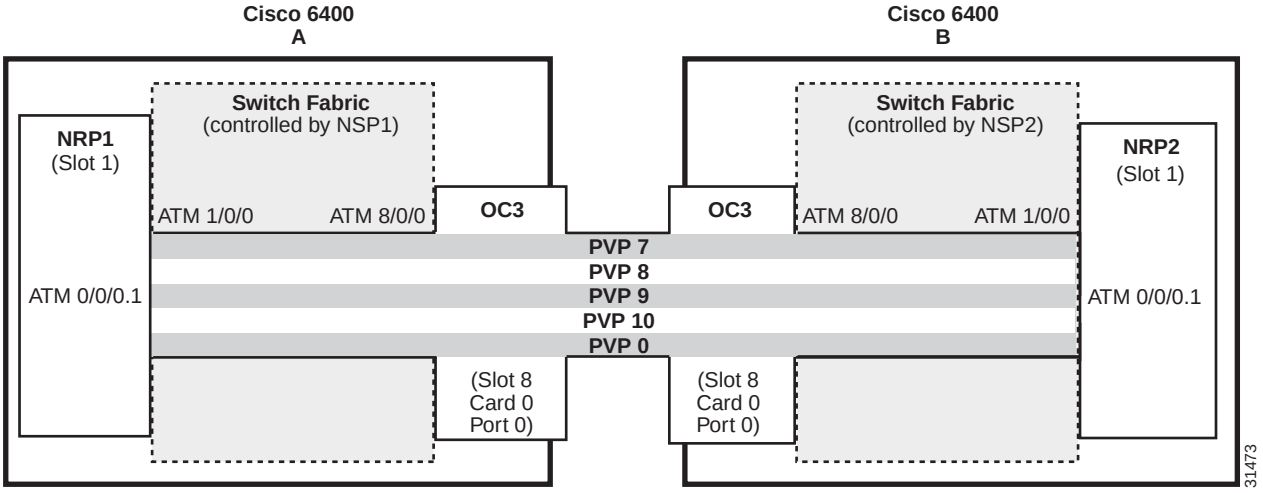
```
NSP(config-if)# atm pvp 10 interface  ATM2/0/0 10
NSP(config-if)# atm pvp 0 interface  ATM2/0/0 0
```

Note This example uses the default control channel PVC 0/32. You can also use a channel within the configured VPI range by using the **tag-switching atm control-vc** interface configuration command on the NRPs. For example, if you want to use the control channel PVC 7/32, then enter **tag-switching atm control-vc 7 32** on both NRP1 and NRP2.

VPI Range Example: Configuring and Connecting Edge LSRs in Separate Cisco 6400s

In this example, two NRPs are configured as Edge LSRs in the separate Cisco 6400s. The Edge LSRs are connected to each other through a VPI range through the MPLS network, as shown in Figure 3-4.

Figure 3-4 VPI Range Between Two NRPs in Different Cisco 6400s



The following example shows the configuration for NRP1 in Slot 1 of Cisco 6400 A:

```
NRP1# configure terminal
NRP1(config)# ip cef
NRP1(config)# tag-switching ip
NRP1(config)# interface ATM0/0/0.1 tag-switching
NRP1(config-if)# ip unnumbered Loopback0
NRP1(config-if)# tag-switching atm vpi 7-10
NRP1(config-if)# tag-switching ip
```

The following example shows the configuration for NRP2 in Slot 1 of Cisco 6400 B:

```
NRP2# configure terminal
NRP2(config)# ip cef
NRP2(config)# tag-switching ip
NRP2(config)# interface ATM0/0/0.1 tag-switching
NRP2(config-if)# ip unnumbered Loopback0
NRP2(config-if)# tag-switching atm vpi 7-10
NRP2(config-if)# tag-switching ip
```

To complete the VPI range connection between NRP1 and NRP2 in Figure 1, the NSPs must be configured to set the path through the switch fabric and node line cards (NLCs). PVP 0 is used to set up the control channels.

The following example shows the VP-switch configuration for NSP1 in Cisco 6400 A:

```
NSP# configure terminal
NSP(config)# interface ATM1/0/0
NSP(config-if)# atm pvp 7 interface  ATM8/0/0 7
NSP(config-if)# atm pvp 8 interface  ATM8/0/0 8
NSP(config-if)# atm pvp 9 interface  ATM8/0/0 9
NSP(config-if)# atm pvp 10 interface  ATM8/0/0 10
NSP(config-if)# atm pvp 0 interface  ATM8/0/0 0
```

The following example shows the VP-switch configuration for NSP2 in Cisco 6400 B:

```
NSP# configure terminal
NSP(config)# interface ATM1/0/0
NSP(config-if)# atm pvp 7 interface  ATM8/0/0 7
NSP(config-if)# atm pvp 8 interface  ATM8/0/0 8
NSP(config-if)# atm pvp 9 interface  ATM8/0/0 9
NSP(config-if)# atm pvp 10 interface  ATM8/0/0 10
NSP(config-if)# atm pvp 0 interface  ATM8/0/0 0
```

Note This example uses the default control channel PVC 0/32. You can also use a channel within the configured VPI range by using the **tag-switching atm control-vc** interface configuration command on the NRPs. For example, if you want to use the control channel PVC 7/32, then enter **tag-switching atm control-vc 7 32** on both NRP1 and NRP2.

MPLS Virtual Private Networks

For general MPLS VPN configuration tasks, examples, and command references, see the "Multiprotocol Label Switching" chapter in the *Cisco IOS Switching Services Configuration Guide*.

In addition to these configurations, you must configure the NSP to create paths through the switch fabric of the Cisco 6400. The switch fabric provides connectivity between the NRPs and the external ports on the node line cards (NLCs). For general configuration tasks, examples, and command references for configuring paths through the switch fabric, see the "Configuring Virtual Connections" chapter in the *ATM Switch Router Software Configuration Guide*.

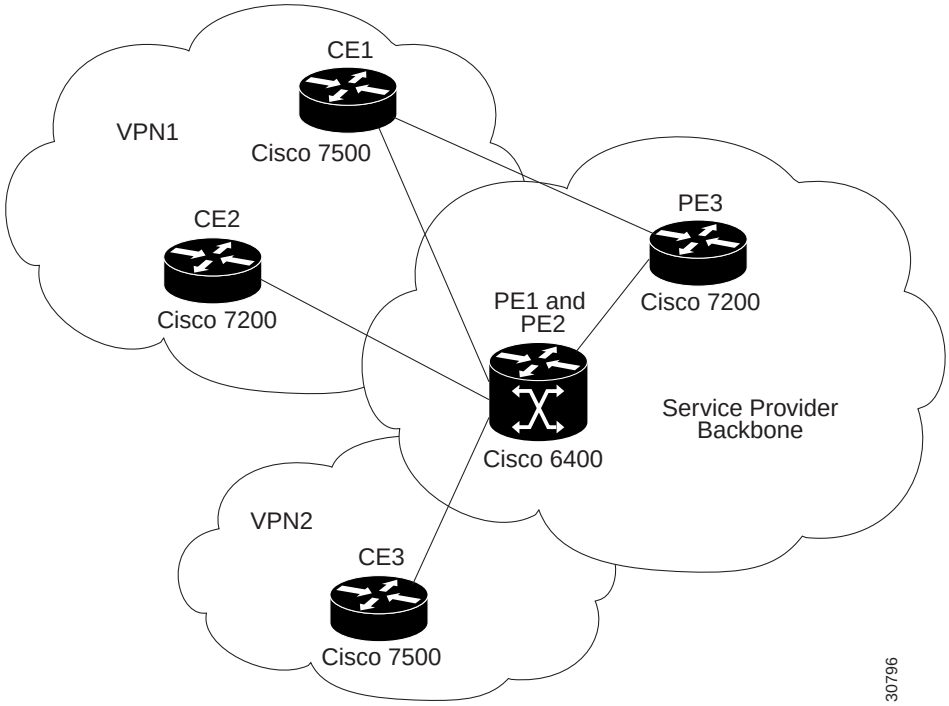
The examples in this section illustrate the configurations necessary to enable MPLS VPN on a Cisco 6400.

Basic MPLS VPN Configuration Example

This section presents a basic Cisco 6400 MPLS VPN configuration. As shown in Figure 3-5, three customer edge (CE) routers are connected to the service provider backbone through three provider edge (PE) routers. Two of the PE routers are NRPs in the Cisco 6400, while the third PE router is a Cisco 7200. CE1 uses dual homing with PE1 and PE3.

CE1 and CE2 are devices in VPN1, while CE3 is in VPN2. PE1, or NRP1 in the Cisco 6400, handles the CE1 portion of VPN1. PE2, or NRP2 in the Cisco 6400, handles VPN2 as well as the CE2 portion of VPN1.

Figure 3-5 Basic Cisco 6400 MPLS VPN Topology

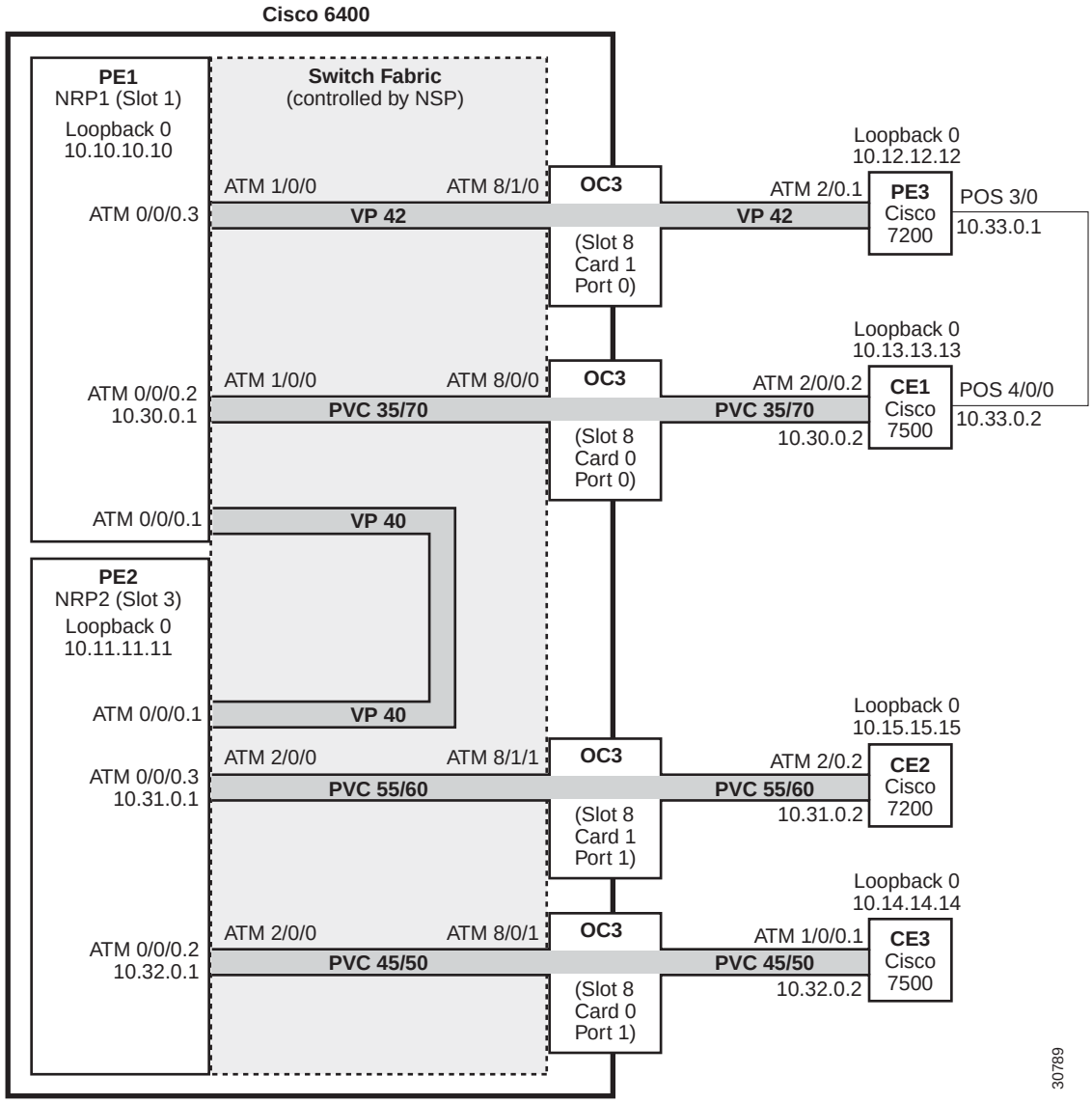


To enable a Cisco 6400 NRP to participate in a VPN, you must configure the NSP to create paths from the NRP through the Cisco 6400 switch fabric. The switch fabric provides the only connection between the NRP and an external port on a network line card (NLC). The switch fabric also provides the only connection between NRPs in the same Cisco 6400. Figure 3-6 shows a detailed schematic of the configuration used in the topology shown in Figure 3-5.

As shown in the accompanying configurations, you can use routed (in compliance with RFC 1483) PVCs for the CE to PE connections, as long as the CE router is capable of performing routing in compliance with RFC 1483 (aal5snap).

Note Each NRP in a Cisco 6400 is capable of handling multiple VPNs.

Figure 3-6 Detailed Schematic of the MPLS VPN Configuration Shown in Figure 3-5



PE1: Cisco 6400 NRP1

PE1 in Figure 3-6 is connected to PE3, through VP 42, and CE1, through PVC 35/70. In addition, PE1 and PE2, both NRPs in the same Cisco 6400, are connected to each other through VP40.

The following example shows the complete configuration for PE1 (Cisco 6400 NRP1):

```
!
ip cef
ip classless
!
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
 no ip directed-broadcast
!
```

```
!The following fragment defines a VPN routing/forwarding (VRF) instance on PE1
!and imports routes from VPN2 to the VRF VPN1 routing table.
!
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 route-target import 200:1
no tag-switching aggregate-statistics
!
!The following fragment creates VP 40 and VP 42 through the MPLS cloud.
!
interface ATM0/0/0.1 tag-switching
 ip unnumbered Loopback0
 no ip directed-broadcast
 ip split-horizon
 atm pvc 40 40 0 aal5snap
 tag-switching atm vp-tunnel 40
 tag-switching ip
!
interface ATM0/0/0.3 tag-switching
 ip unnumbered Loopback0
 no ip directed-broadcast
 ip split-horizon
 atm pvc 42 42 0 aal5snap
 tag-switching atm vp-tunnel 42
 tag-switching ip
!
!The following fragment associates an interface with a VRF on PE1.
!
interface ATM0/0/0.2 point-to-point
 ip vrf forwarding vpn1
 ip address 10.30.0.1 255.255.0.0
 no ip directed-broadcast
 ip split-horizon
 atm pvc 70 35 70 aal5snap
!
!The following fragment configures Interior Gateway Protocol (IGP) routing on PE1.
!
router ospf 100
 passive-interface ATM0/0/0.2
 network 10.0.0.0 0.255.255.255 area 100
!
!The following fragment configures Routing Information Protocol (RIP)
!between PE1 and CE1. You can also use Border Gateway Protocol (BGP) or
!static routing instead of RIP.
!
router rip
 version 2
 !
 address-family ipv4 vrf vpn1
 version 2
 redistribute bgp 100 metric transparent
 network 10.30.0.0
 no auto-summary
 exit-address-family
!
!The following fragment configures internal BGP sessions among the PE routers.
!
router bgp 100
 no synchronization
 no bgp default ipv4-unicast
 neighbor 10.11.11.11 remote-as 100
 neighbor 10.11.11.11 update-source Loopback0
```

```
 neighbor 10.12.12.12 remote-as 100
 neighbor 10.12.12.12 update-source Loopback0
 !
 address-family ipv4 vrf vpn1
 redistribute rip
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.11.11.11 activate
 neighbor 10.11.11.11 send-community extended
 neighbor 10.12.12.12 activate
 neighbor 10.12.12.12 send-community extended
 exit-address-family
!
```

PE2: Cisco 6400 NRP2

PE2 in Figure 3-6 is connected to CE2, through PVC 55/60, and CE3, through PVC 45/50. In addition, PE1 and PE2, both NRPs in the same Cisco 6400, are connected to each other through VP40.

The following example shows the complete configuration for PE2 (Cisco 6400 NRP2):

```
!
ip cef
ip classless
!
interface Loopback0
 ip address 10.11.11.11 255.255.255.255
 no ip directed-broadcast
!
!The following fragment defines the VRF instances on PE2. The fragment also
!imports the routes from VPN2 to the VRF VPN1 routing table and imports the
!routes from VPN1 to the VRF VPN2 routing table.
!
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 route-target import 200:1
!
ip vrf vpn2
 rd 200:1
 route-target export 200:1
 route-target import 200:1
 route-target import 100:1
!
!The following fragment creates VP 40 through the MPLS cloud.
!
interface ATM0/0/0.1 tag-switching
 ip unnumbered Loopback0
 no ip directed-broadcast
 ip split-horizon
 atm pvc 40 40 0 aal5snap
 tag-switching atm vp-tunnel 40
 tag-switching ip
!
!The following fragment associates interfaces with VRFs on PE2.
!
interface ATM0/0/0.2 point-to-point
 ip vrf forwarding vpn2
 ip address 10.32.0.1 255.255.0.0
```

```
 no ip directed-broadcast
 ip split-horizon
 atm pvc 50 45 50 aal5snap
!
interface ATM0/0/0.3 point-to-point
 ip vrf forwarding vpn1
 ip address 10.31.0.1 255.255.0.0
 no ip directed-broadcast
 ip split-horizon
 atm pvc 60 55 60 aal5snap
!
!The following fragment configures IGP routing on PE2.
!
router ospf 100
 passive-interface ATM0/0/0.2
 passive-interface ATM0/0/0.3
 network 10.11.0.0 0.0.255.255 area 100
!
!The following fragment configures RIP between PE2 and CE2, as well as
!between PE2 and CE3. You can also use Border Gateway Protocol (BGP) or
!static routing instead of RIP.
!
router rip
 version 2
 !
 address-family ipv4 vrf vpn2
 version 2
 redistribute bgp 100 metric transparent
 network 10.32.0.0
 no auto-summary
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 version 2
 redistribute bgp 100 metric transparent
 network 10.31.0.0
 no auto-summary
 exit-address-family
!
!The following fragment configures internal BGP sessions among the PE routers.
!
router bgp 100
 no synchronization
 no bgp default ipv4-unicast
 neighbor 10.10.10.10 remote-as 100
 neighbor 10.10.10.10 update-source Loopback0
 neighbor 10.12.12.12 remote-as 100
 neighbor 10.12.12.12 update-source Loopback0
 !
 address-family ipv4 vrf vpn2
 redistribute rip
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf vpn1
 redistribute rip
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.10.10.10 activate
 neighbor 10.10.10.10 send-community extended
```

```
 neighbor 10.12.12.12 activate
 neighbor 10.12.12.12 send-community extended
 exit-address-family
!
```

PE1 and PE2 Connectivity: Cisco 6400 NSP

The following example shows the configuration necessary for the PE Cisco 6400 NSP to create the paths in the switch fabric between the NRPs and the OC3 line cards shown in Figure 3-6.

```
!The following fragment creates VP 42 between
!an OC3 (slot 8, card 1, port 0) and NRP1.
!
interface ATM8/1/0
 atm pvp 42  interface  ATM1/0/0 42
!
!The following fragment creates PVC 35/70 between
!an OC3 (slot 8, card 0, port 0) and NRP1.
!
interface ATM8/0/0
 atm pvc 35 70  interface  ATM1/0/0 35 70
!
!The following fragment creates VP 40 between NRP1 in Slot 1
!and NRP2 in Slot 3.:
!
interface ATM3/0/0
 atm pvp 40  interface  ATM1/0/0 40
!
!The following fragment creates PVC 55/60 between
!an OC3 (slot 8, card 1, port 1) and NRP2.
!
interface ATM8/1/1
 atm pvc 55 60  interface  ATM3/0/0 55 60
!
!The following fragment creates PVC 45/50 between
!an OC3 (slot 8, card 0, port 1) and NRP2.
!
interface ATM8/0/1
 atm pvc 45 50  interface  ATM3/0/0 45 50
!
```

PE3: Cisco 7200

PE3 in Figure 3-6 is connected to PE1, through VP 42, and CE1, through a packet over SONET (POS) link.

The following example shows the complete configuration for PE3 (Cisco 7200):

```
ip cef
ip classless
!
interface Loopback0
 ip address 10.12.12.12 255.255.255.255
 no ip directed-broadcast
!
!The following fragment defines the VRF instances on PE3.
!
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 route-target import 200:1
```

```
isdn voice-call-failure 0
!
!The following fragment associates a POS interface with a VRF on PE3.
!
interface POS3/0
 ip vrf forwarding vpn1
 ip address 10.33.0.1 255.255.0.0
 no ip directed-broadcast
 no keepalive
 clock source internal
!
!The following fragment creates VP 42 through the MPLS cloud.
!
interface ATM2/0.1 tag-switching
 ip unnumbered Loopback0
 no ip directed-broadcast
 ip split-horizon
 atm pvc 42 42 0 aal5snap
 tag-switching atm vp-tunnel 42
 tag-switching ip
!
!The following fragment configures IGP routing on PE3.
!
router ospf 100
 passive-interface POS3/0
 network 10.12.0.0 0.0.255.255 area 100
!
!The following fragment configures RIP between PE3 and CE1.
!You can also use BGP or static routing instead of RIP.
!
router rip
 version 2
 !
 address-family ipv4 vrf vpn1
 version 2
 redistribute bgp 100 metric transparent
 network 10.33.0.0
 no auto-summary
 exit-address-family
!
!The following fragment configures internal BGP sessions
!among the PE routers.
!
router bgp 100
 no synchronization
 no bgp default ipv4-unicast
 neighbor 10.10.10.10 remote-as 100
 neighbor 10.10.10.10 update-source Loopback0
 neighbor 10.11.11.11 remote-as 100
 neighbor 10.11.11.11 update-source Loopback0
 !
 address-family ipv4 vrf vpn1
 redistribute rip
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.10.10.10 activate
 neighbor 10.10.10.10 send-community extended
 neighbor 10.11.11.11 activate
 neighbor 10.11.11.11 send-community extended
 exit-address-family
!
```

CE1: Cisco 7500

CE1 in Figure 3-6 is connected to PE1, through PVC 35/70, and PE3, through a packet over SONET (POS) link.

The following example shows the configuration for CE1 (Cisco 7500):

```
!
ip cef
ip classless
!
interface Loopback0
 ip address 10.13.13.13 255.255.255.255
 no ip directed-broadcast
!
!The following fragment creates the POS link between CE1 and PE3.
!
interface POS4/0/0
 ip address 10.33.0.2 255.255.0.0
 no ip directed-broadcast
 no ip route-cache distributed
 no keepalive
 clock source internal
!
!The following fragment creates PVC 35/70.
!
interface ATM2/0/0.2 point-to-point
 ip address 10.30.0.2 255.255.0.0
 no ip directed-broadcast
 ip split-horizon
 atm pvc 70 35 70 aal5snap
!
!The following fragment configures RIP on CE1.
!You can also use BGP or static routing instead of RIP:
!
router rip
 version 2
 network 10.13.0.0
 network 10.30.0.0
 network 10.33.0.0
!
```

CE2: Cisco 7200

CE2 in Figure 3-6 is connected to PE2, through PVC 55/60.

The following example shows the configuration for the CE2 (Cisco 7200):

```
!
ip cef
ip classless
!
interface Loopback0
 ip address 10.15.15.15 255.255.255.255
 no ip directed-broadcast
!
!The following fragment creates PVC 55/60.
!
interface ATM2/0.2 point-to-point
 ip address 10.31.0.2 255.255.0.0
 no ip directed-broadcast
 ip split-horizon
 atm pvc 60 55 60 aal5snap
```

```
!
!The following fragment configures RIP on CE2.
!You can also use BGP or static routing instead of RIP:
!
router rip
 version 2
 network 10.15.0.0
 network 10.31.0.0
!
```

CE3: Cisco 7500

CE3 in Figure 3-6 is connected to PE2, through PVC 45/50.

The following example shows the configuration for CE3 (Cisco 7500):

```
!
ip cef
ip classless
!
interface Loopback0
 ip address 10.14.14.14 255.255.255.255
 no ip directed-broadcast
!
!The following fragment creates PVC 45/50.
!
interface ATM1/0/0.1 point-to-point
 ip address 10.32.0.2 255.255.0.0
 no ip directed-broadcast
 ip split-horizon
 atm pvc 50 45 50 aal5snap
!
!The following fragment configures RIP on CE3.
!You can also use BGP or static routing instead of RIP.
!
router rip
 version 2
 network 10.14.0.0
 network 10.32.0.0
!
```

Split Horizon and RIP Example

Note Split horizon is disabled by default on ATM interfaces. If you are running RIP in your VPNs, you must enable split horizon.

The following example shows a typical configuration for an ATM subinterface on an NRP:

```
NRP# configure terminal
NRP(config)# interface ATM0/0/0.1 tag-switching
NRP(config-if)# ip unnumbered Loopback0
NRP(config-if)# ip split-horizon
NRP(config-if)# no ip directed-broadcast
NRP(config-if)# atm pvc 40 40 0 aal5snap
NRP(config-if)# tag-switching atm vp-tunnel 40
NRP(config-if)# tag-switching ip
```

CHAPTER 4

Point-to-Point Protocol

This chapter provides restrictions, prerequisites, and tasks for PPP features supported by the Cisco 6400 in Cisco IOS Release 12.2(4)B.

This chapter only describes tasks that are specific to the Cisco 6400 and supplements the following documentation:

Documentation	Relevant Information
"Supported Features" chapter	Includes a complete list of PPP and PPP-related features supported by the Cisco 6400 in Cisco IOS Release 12.2(4)B.
Cisco IOS Wide-Area Networking Configuration Guide	Provides general PPP broadband access overview, configuration, verification, monitoring, and troubleshooting information.
Cisco IOS Dial Technologies Configuration Guide	Provides general PPP overview, configuration, verification, monitoring, and troubleshooting information.

This chapter includes the following sections:

Refer to the "Supported Features" chapter for additional documentation on L2TP features.

Restrictions

PPPoE

- PPPoE is supported on ATM PVCs only.
- The Cisco 6400 cannot initiate dial-out PPPoE sessions.
- PPPoE supports Cisco Express Forwarding (CEF) only. Fastswitching on PPPoE virtual-access interfaces is not supported.

PPPoA

- PPPoA does not support static IP assignments within virtual templates.

PPPoA/PPPoE Autosense on ATM VC with SNAP Encapsulation

- Do not use this feature on a router that initiates PPPoA sessions.
- This feature supports ATM PVCs. Switched virtual circuits (SVCs) are not supported.
- This feature supports only PPPoA sessions that use SNAP or Logical Link Control (LLC) encapsulation. This feature does not support MUX-encapsulated PVCs.

PPPoE Session Count MIB

- The **snmp-server enable traps pppoe** command enables SNMP traps only. It does not support inform requests.

Prerequisites

PPP Scalability

- See the Cisco 6400 Release Notes for memory recommendations.
- In order to gain maximum packet-switching performance, enable Cisco Express Forwarding (CEF) on the virtual-access interface. For information about enabling Cisco Express Forwarding, see the "Configuring Cisco Express Forwarding" chapter in the "Cisco IOS Switching Paths" part of the *Cisco IOS Switching Services Configuration Guide*.

PPPoE Session Count MIB

- The tasks as described in the "PPPoE Session Count MIB" section on page 4-17 assume that you have configured SNMP and PPPoE.

Basic PPPoE Configuration

Note Before performing these tasks, read the Restrictions and Prerequisites sections.

The NRP uses virtual templates to assign PPP features to a PVC. As each PPP session comes online, a virtual access interface is "cloned" from the virtual template. This virtual-access interface inherits the configuration specified in the virtual template. When the virtual template is changed, the changes are automatically propagated to all virtual-access interfaces cloned from that particular virtual template.

After you configure a virtual template for PPPoE, you must configure the PVCs that carry traffic from the NRP to the ATM interfaces. Finally, to allow PPPoE to operate over the virtual-access interface, set the IP maximum transmission unit (MTU) to 1492.

Basic PPPoE configuration consists of the following tasks:

- Task 1: Configuring a Virtual Template for PPPoE
- Task 2: Configuring PPPoE on the ATM Interface
- Task 3: Setting the MTU

Task 1: Configuring a Virtual Template for PPPoE

To configure a virtual template for PPPoE, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vpdn enable`	Enables virtual private dial-up networking.
Step 2	`Router(config)# vpdn-group number`	Selects the VPDN group and enters VPDN group configuration mode.
Step 3	`Router(config-vpdn)# accept dialin pppoe virtual-template number`	Configures the router to accept dial-in PPPoE calls.
Step 4	`Router(config-vpdn)# pppoe limit per-mac number`	(Optional) Limits the number of PPPoE sessions that originate from one MAC address. Default is 100.
Step 5	`Router(config-vpdn)# pppoe limit per-vc number`	(Optional) Limits the number of PPPoE sessions that can be established on a virtual circuit. Default is 100.
Step 6	`Router(config-vpdn)# exit`	Returns to global configuration mode.
Step 7	`Router(config)# virtual-template template-number pre-clone number`	(Optional) Creates “pre-cloned” virtual-access interfaces equal to the expected maximum number of concurrent PPPoE sessions.[1]

1. Instead of creating virtual-access interfaces on demand, the system can be configured to create and save a number of *pre-cloned* virtual-access interfaces to a private PPPoE list. This cloning procedure reduces the CPU workload while PPPoE sessions are established.

Task 2: Configuring PPPoE on the ATM Interface

To configure PPPoE on the ATM interface, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface atm 0/0/0 [.subinterface-number {multipoint | point-to-point}]`	Specifies the ATM interface and optional subinterface.
Step 2	`Router(config-if)# pvc [name] vpi/vci`	Configures the PVC.
Step 3	`Router(config-atm-vc)# encapsulation aal5snap`	Configures SNAP encapsulation.
Step 4	`Router(config-atm-vc)# protocol pppoe`	Selects PPPoE as the protocol for the PVC.

You can also configure PPPoE in a VC class and apply this VC class to an ATM VC, subinterface, or interface. For information about configuring a VC classes, see the "Permanent Virtual Circuits" section in the "Basic NRP Configuration" chapter of the *Cisco 6400 Software Setup Guide*. Also see the "Example: PPPoE Configuration Using a VC Class" section on page 4-6.

Task 3: Setting the MTU

To allow PPPoE to operate over the virtual-access interface, set the maximum transmission unit (MTU) to 1492. To set the MTU, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface virtual-template` *number*	Selects the virtual-access interface to be configured.
Step 2	`Router(config-if)# mtu 1492`	Sets the MTU to 1492.

Verifying PPPoE

Step 1 Enter the **show vpdn** EXEC command. The output shows PPPoE session information (see Table 4-1). Confirm that the virtual-access interface status (VASt) is up.

```
Router# show vpdn

PPPOE Tunnel and Session

Session count: 1

PPPoE Session Information
SID         RemMAC          LocMAC       Intf    VASt    OIntf   VC
1          0010.54db.bc38  0050.7327.5dc3  Vi1     UP      AT0/0/0 0/40
```

Table 4-1 show vpdn Field descriptions

Field	Description
SID	Session ID for the PPPoE session
RemMAC	MAC address of the host
LocMAC	MAC address of the ATM interface
Intf	Virtual-access interface associated with the PPP session
VASt	State of the virtual-access interface
OIntf	Outgoing interface
VC	Virtual circuit on which PPP session flows

Step 2 Enter the **show atm pvc** privileged EXEC command. The last line of the output, "PPPOE enabled," confirms that PPPoE is enabled on this VC.

```
Router# show atm pvc 40
ATM0/0/0.2: VCD: 1, VPI: 0, VCI: 40
UBR, PeakRate: 155000
AAL5-LLC/SNAP, etype:0x0, Flags: 0xC20, VCmode: 0x0
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s), OAM retry
```

```
frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Disabled
OAM VC state: Not Managed
ILMI VC state: Not Managed
InARP frequency: 15 minutes(s)
InPkts: 100, OutPkts: 51, InBytes: 4692, OutBytes: 2294
InPRoc: 48, OutPRoc: 51, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 52, OutAS: 0
OAM cells received: 0
F5 InEndloop: 0, F5 InSegloop: 0, F5 InAIS: 0, F5 InRDI: 0
F4 InEndloop: 0, F4 InSegloop: 0, F4 InAIS: 0, F4 InRDI: 0
OAM cells sent: 0
F5 OutEndloop: 0, F5 OutSegloop: 0, F5 OutRDI: 0
F4 OutEndloop: 0, F4 OutSegloop: 0, F4 OutRDI: 0
OAM cell drops: 0
Status: UP
➔ PPPOE enabled.
```

Examples: Configuring PPPoE

This section provides the following PPPoE configuration examples:

- Example: PPPoE Configuration on a PVC
- Example: PPPoE Configuration Using a VC Class
- Example: Concurrent PPPoE and Bridging

Example: PPPoE Configuration on a PVC

In the following example, PPPoE is enabled directly on a PVC:

```
!
vpdn enable
!
vpdn-group 1
 accept dialin pppoe virtual-template 1
!
virtual-template 1 pre-clone 500
!
interface atm 2/0.1 multipoint
 pvc 0/60
  encapsulation aal5snap
  protocol pppoe
!
ip cef
!
interface virtual-template 1
 ip address 10.0.1.2 255.255.255.0
 mtu 1492
 ip route-cache cef
 !
```

Example: PPPoE Configuration Using a VC Class

In the following example, PPPoE is configured on a VC class called “users.” This VC class is then applied to a particular PVC:

```
!
vpdn enable
!
vpdn-group 1
 accept dialin pppoe virtual-template 1
!
virtual-template 1 pre-clone 500
!
interface atm 2/0.1 multipoint
 pvc 0/60
  class users
  !
vc-class atm users
 encapsulation aal5snap
 protocol pppoe
 !
ip cef
!
interface virtual-template 1
 ip address 10.0.1.2 255.255.255.0
 mtu 1492
 ip route-cache cef
 !
```

Example: Concurrent PPPoE and Bridging

PPPoE can operate concurrently with bridging on an ATM interface. This allows PPPoE to operate on one or more specific traffic protocols, leaving other protocols to be bridged.

In the following example, both PPPoE and bridging are configured to operate concurrently on the same DSL link:

```
!
vpdn enable
!
vpdn-group 1
 accept dialin pppoe virtual-template 1
 !
virtual-template 1 pre-clone 500
!
bridge 1 protocol ieee
bridge 1 route ip
!
interface atm 2/0.1 multipoint
 bridge-group 1
 pvc 0/60
  encapsulation aal5snap
  protocol pppoe
  !
ip cef
!
interface virtual-template 1
 ip address 10.0.1.2 255.255.255.0
 mtu 1492
 ip route-cache cef
 !
```

Monitoring and Maintaining PPPoE

Use the following commands to monitor and maintain PPPoE:

Command	Purpose
show atm pvc	Displays ATM PVC and traffic information, including PPPoE status.
show vpdn	Displays PPPoE session information, including MAC addresses and virtual-access interfaces.
show vpdn session packet	Displays PPPoE session statistics.
show vpdn session all	Displays PPPoE session information for each session ID.
show vpdn tunnel	Displays PPPoE session count for the tunnel.

Basic PPPoA Configuration

Note Before performing these tasks, read the "Restrictions" section on page 4-2.

The NRP uses virtual templates to assign PPP features to a PVC. As each PPP session comes online, a virtual access interface is "cloned" from the virtual template. This virtual-access interface inherits the configuration specified in the virtual template. When the virtual template is changed, the changes are automatically propagated to all virtual-access interfaces cloned from that particular virtual template.

After you configure a virtual template for PPPoA, you must configure the PVCs that carry traffic from the NRP to the ATM interfaces.

While you can use a local username database for authentication, large-scale deployment of PPP user services requires the use of a central database, such as TACACS+ or RADIUS to ease the configuration burden. RADIUS or TACACS+ servers, collectively known as authentication, authorization, and accounting (AAA) servers for PPPoA (and other media), contain the per-user configuration database, including password authentication and authorization information. For more information about AAA, see the "Authentication, Authorization, and Accounting (AAA)" chapter in the *Cisco IOS Security Configuration Guide.*

Basic PPPoA configuration consists of the following tasks:

- Task 1: Configuring a Virtual Template for PPPoA
- Task 2: Configuring PPPoA on a PVC
- Task 3: Configuring Authentication

Task 1: Configuring a Virtual Template for PPPoA

To configure a virtual template for PPPoA, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface virtual-template` *number*	Associates a virtual template with a virtual template interface.
Step 2	`Router(config-if)# ip unnumbered fastethernet 0/0/0`	Enables IP on the interface without assigning a specific IP address.
Step 3	`router(config-if)# peer default ip address {pool [`*poolname*`] | dhcp }`	Specifies a dynamic IP address assignment method, either from an IP address pool or a DHCP server.
Step 4	`Router(config-if)# ppp authentication {pap | chap} [pap | chap]`	Selects the authentication protocol and optional secondary protocol.
Step 5	`Router(config-if)# exit`	Returns to global configuration mode.
Step 6	`Router(config)# ip local pool` *poolname low-ip-address* `[`*high-ip-address*`]`	(Optional) Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.
Step 7	`Router(config)# ip dhcp-server {`*ip-address* `|` *name*`}`	(Optional) Specifies which DHCP server to use on your network.

Caution Do not use a static IP assignment within a virtual template; routing problems can occur. Always enter the **ip unnumbered** command when configuring a virtual template.

To configure a different class of users on the same router, provision a separate virtual template interface. You can configure up to 25 virtual templates.

Examples: Configuring a Virtual Template for PPPoA

In the following example, all PPPoA VCs (users) cloned from virtual template 1 will use CHAP authentication and will be allocated an IP address from the pool named “telecommuters” configured on the router. In addition, the local end of the PPPoA connection is running without an IP address (recommended). Instead, the IP address of the FastEthernet interface is used for addressability:

```
!
interface virtual-template 1
 ip unnumbered fastethernet 0/0/0
 peer default ip address pool telecommuters
 ppp authentication chap
 !
local pool telecommuters 10.36.1.1 10.36.1.254
!
```

In the following example, all PPPoA VCs cloned from Virtual-Template 2 use PAP authentication over CHAP and are allocated an IP address from a DHCP server:

```
!
interface Virtual-Template 2
 ip unnumbered fastethernet 0/0/0
 peer default ip address dhcp
```

```
 ppp authentication pap chap
 !
ip dhcp-server 10.5.20.149
!
```

Task 2: Configuring PPPoA on a PVC

To configure PPPoA on a PVC, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface atm 0/0/0 [.subinterface-number {multipoint | point-to-point}]`	Specifies the ATM interface and optional subinterface.
Step 2	`Router(config-if)# pvc [name] vpi/vci`	Configures a new ATM PVC by assigning a name (optional) and VPI/VCI numbers.
Step 3	`Router(config-if-atm-vc)# encapsulation aal5mux ppp virtual-Template number`	Configures the ATM adaptation layer (AAL) and encapsulation type, and configures a PVC to use a virtual-template as the default PPP interface configuration.

You can also configure PVCs by using VC classes and PVC discovery. For more information, see the "Permanent Virtual Circuits" section in the "Basic NRP Configuration" chapter of the *Cisco 6400 Software Setup Guide*.

Task 3: Configuring Authentication

To configure authentication for PPPoA, see the "PPP Authentication" section on page 4-10.

Example: Basic PPPoA Configuration

The following example shows a typical PPPoA configuration using a RADIUS authentication server:

```
!
interface virtual-template 1
 ip unnumbered fastethernet 0/0/0
 peer default ip address pool telecommuters
 ppp authentication chap
 !
ip local pool telecommuters 10.36.1.1 10.36.1.254
!
aaa new-model
aaa authentication ppp default radius
radius-server host 172.31.5.96
radius-server key foo
radius-server attribute nas-port format d
!
interface atm 0/0/0.40 multipoint
 pvc 0/50
  encapsulation aal5mux ppp virtual-template 1
  !
 pvc 0/51
  encapsulation aal5mux ppp virtual-template 1
  !
```

Verifying and Troubleshooting PPPoA

Step 1 Enter the **show atm pvc ppp** privileged EXEC command to display the PPPoA characteristics of all PVCs on the ATM interface:

```
Router# show atm pvc ppp
                 VCD /
ATM Int.         Name          VPI    VCI  Type    VCSt  VA    VASt IP Addr
0/0/0            1               0     33   PVC      UP   1    DOWN 10.123.1.1
0/0/0            foo             0     34   PVC      UP   2    DOWN 10.123.1.1
```

The "VA" column shows the virtual-access interface used for this particular PPPoA session.

Step 2 Enter the **show interface virtual-access** privileged EXEC command to display the PPP specific characteristics of the session:

```
Router# show interface virtual-access 2
Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Internet address is 10.123.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive not set
  DTR is pulsed for 5 seconds on reset
  LCP Open
  Open: IPCP
  Bound to ATM0/0/0 VCD: 2, VPI: 0, VCI: 34
  Cloned from virtual-template: 1
  Last input 01:04:26, output never, output hang never
  Last clearing of "show interface" counters 5d02h
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     782 packets input, 30414 bytes, 0 no buffer
     Received 3 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     395 packets output, 5540 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
```

The lines highlighted in the previous example show the layer 3 protocols enabled on this interface, the VPI and VCI numbers, and the master virtual template from which this virtual access interface was cloned.

PPP Authentication

Large-scale deployment of PPP user services requires the use of a central database, such as TACACS+ or RADIUS to ease the configuration burden. RADIUS or TACACS+ servers, collectively known as authentication, authorization, and accounting (AAA) servers for PPP over ATM (and other media), contain the per-user configuration database, including password authentication and authorization information. For more information about AAA, see the "Authentication, Authorization, and Accounting (AAA)" chapter in the *Cisco IOS Security Configuration Guide*.

PPP authentication configuration consists of the following tasks:

- Task 1: Selecting the PPP Authentication Method, page 4-11
- Task 2 (Option 1): Configuring Communication with a RADIUS Server, page 4-12
- Task 2 (Option 2): Configuring Communication with a TACACS+ Server, page 4-12

Task 1: Selecting the PPP Authentication Method

To select the PPP authentication method, complete the following steps in global configuration mode:

	Command	Description
Step 1	`Router(config)# aaa new-model`	Enables the AAA access control model.
Step 2	`Router(config)# aaa authentication ppp {default | list-name} method1 [method2...]`	Specifies one or more authentication methods for use on interfaces running PPP.

The *list-name* option refers to the name of this particular method list (or default, if it is the default list). The authentication *method* options are local, RADIUS, or TACACS+.

Example: Selecting the TACACS+ and RADIUS PPP Authentication Methods

In the following example, virtual template 3 is configured to use TACACS+ before RADIUS, and virtual template 4 is configured to use RADIUS before local authentication:

```
!
aaa new-model
aaa authentication ppp list1 tacacs+ radius
aaa authentication ppp list2 radius local
!
interface virtual-template 3
 ip unnumbered fastethernet 0/0/0
 ppp authentication chap list1
 !
interface virtual-template 4
 ip unnumbered fastethernet 0/0/0
 ppp authentication chap list2
 !
```

Example: Selecting the Local PPP Authentication Method

In the following example, only the local username database is used for authentication:

```
!
aaa new-model
aaa authentication ppp default local
!
```

Task 2 (Option 1): Configuring Communication with a RADIUS Server

Note This task is required if you configured the RADIUS authentication method.

To configure the NRP to communicate properly with a RADIUS server, complete the following steps in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number]`	Specifies a RADIUS server host. You do not have to specify the authentication and accounting port numbers because they default to 1645 and 1646, respectively.
Step 2	`Router(config)# radius-server key key`	Sets the encryption key to match that used on the RADIUS server.
Step 3	`Router(config)# radius-server attribute nas-port format d`	Selects the ATM VC extended format (**d**) for the NAS port field.

Example: Configuring Communication with a RADIUS Server

In the following example, a RADIUS server is enabled and identified, and the NAS port field is set to ATM VC extended format:

```
!
aaa new-model
aaa authentication ppp default radius
!
radius-server host 172.31.5.96 auth-port 1645 acct-port 1646
radius-server key foo
radius-server attribute nas-port format d
!
```

Task 2 (Option 2): Configuring Communication with a TACACS+ Server

Note This task is required if you configured the TACACS+ authentication method.

To configure the NRP to communicate properly with a TACACS+ server, complete the following steps in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# tacacs-server host {hostname | ip-address} [single-connection] [port integer] [timeout integer] [key string]`	Specifies a TACACS+ server host.
Step 2	`Router(config)# tacacs-server key key`	Sets the encryption key to match that used on the TACACS+ daemon.

Example: Configuring Communication with a TACACS+ Server

In the following example, a TACACS+ server is enabled and identified:

```
!
aaa new-model
aaa authentication ppp default tacacs+
!
tacacs-server host 172.31.5.96
tacacs-server key foo
!
```

PPPoA/PPPoE Autosense on ATM VC with SNAP Encapsulation

Note Before performing these tasks, read the "Restrictions" section on page 4-2.

PPPoA/PPPoE autosense enables the network access server (NAS) to distinguish between incoming PPPoA and PPPoE sessions, and to allocate resources on demand for both PPP types. You can configure PPPoA/PPPoE autosense on a single PVC or on a VC class that can be applied to all PVCs on an ATM interface.

PPPoA/PPPoE autosense provides resource allocation on demand. For each PVC configured for both PPPoA and PPPoE, certain resources (including one virtual-access interface) are allocated upon configuration, regardless of the existence of a PPPoA or PPPoE session on that PVC. With PPPoA/PPPoE autosense, resources are allocated for PPPoA and PPPoE sessions only when a client initiates a session, reducing overhead on the network access server (NAS).

Note Whenever possible, configure PPPoA and PPPoE to use the same virtual template. Using separate virtual templates leads to the inefficient use of virtual access because the maximum number of virtual-access interfaces will have to be precloned twice: once for PPPoE and once for PPPoA. If PPPoA and PPPoE use the same virtual template, the maximum number of virtual-access interfaces can be precloned once and used for PPPoA and PPPoE as needed.

Option 1: Configuring PPPoA/PPPoE Autosense on a PVC

To configure PPPoA/PPPoE autosense on a PVC, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface atm 0/0/0[.subinterface-number] {multipoint | point-to-point | tag-switching}`	Specifies the ATM interface and optional subinterface.
Step 2	`Router(config-subif)# pvc [name] vpi/vci`	Configures a PVC on the ATM interface or subinterface.
Step 3	`Router(config-if-atm-vc)# encapsulation aal5autoppp Virtual-Template number`	Configures PPPoA/PPPoE autosense on the PVC. Also specifies the virtual template interface to clone the new virtual access interfaces for PPPoA sessions on this PVC.

Example: Configuring PPPoA/PPPoE Autosense on a PVC

In the following example, the NAS is configured with PPPoA/PPPoE autosense on PVC 30/33.

```
!
! Configure PPPoA/PPPoE autosense
!
interface ATM 0/0/0.33 multipoint
  pvc 30/33
   encapsulation aal5autoppp Virtual-Template1
!
! Configure PPPoE
!
vpdn enable
vpdn-group 1
  accept dialin pppoe virtual-template 1
!
ip cef
interface virtual-template 1
  ip unnumbered fastethernet 0/0/0
  mtu 1492
  ip route-cache cef
!
! Enable precloning for virtual-template 1
!
virtual-template 1 pre-clone 2000
!
```

Option 2: Configuring PPPoA/PPPoE Autosense on a VC Class

Note Virtual access interfaces for PPPoE sessions are cloned from the virtual template interface specified in the VPDN group.

To configure PPPoA/PPPoE autosense on a VC class, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vc-class atm vc-class-name`	Creates and names a map class.
Step 2	`Router(config-vc-class)# encapsulation aal5autoppp Virtual-Template number`	Configures PPPoA/PPPoE autosense on the VC class. Also specifies the virtual template interface to use to clone the new virtual access interfaces for PPPoA sessions on this PVC.
Step 3	`Router(config-vc-class)# exit`	Returns to global configuration mode.
Step 4	`Router(config)# interface atm 0/0/0[.subinterface-number] {multipoint | point-to-point | tag-switching}`	Specifies the ATM interface and optional subinterface.
Step 5	`Router(config-subif)# class-int vc-class-name`	Applies the VC class to all VCs on the ATM interface or subinterface.

Example: Configuring PPPoA/PPPoE Autosense on a VC Class

In the following example, the NAS is configured with PPPoA/PPPoE autosense on the VC class called "MyClass." MyClass applies the PPPoA/PPPoE autosense feature to all PVCs on the ATM 0/0/0.99 interface:

```
!
! Configure PPPoA/PPPoE autosense
!
vc-class ATM MyClass
  encapsulation aal5autoppp Virtual-Template1
!
interface ATM 0/0/0.99 multipoint
  class-int MyClass
  no ip directed-broadcast
  pvc 20/40
  pvc 30/33
!
! Configure PPPoE
!
vpdn enable
vpdn-group 1
  accept dialin pppoe virtual-template 1
!
ip cef
interface virtual-template 1
  ip unnumbered fastethernet 0/0/0
  mtu 1492
  ip route-cache cef
!
! Enable precloning for virtual-template 1
!
virtual-template 1 pre-clone 2000
!
```

Example: Configuring PPPoA/PPPoE Autosense on Multiple VC Classes and Virtual Templates

In the following example, PPPoA and PPPoE sessions are handled separately by two VC classes and two virtual templates:

```
ip cef
vpdn enable
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
pppoe limit per-mac 1
pppoe limit per-vc 1
!
virtual-template 1 pre-clone 1500
!
interface ATM0/0/0.1 multipoint
no ip directed-broadcast
class-int pppoe
!
interface ATM0/0/0.3 multipoint
no ip directed-broadcast
class-int pppoa
!
interface ATM0/0/0.9 multipoint
ip address 10.16.40.1 255.255.0.0
```

```
no ip directed-broadcast
!
interface Virtual-Template1
ip unnumbered ATM0/0/0.9
ip route-cache cef
no ip directed-broadcast
peer default ip address pool pool-1
ppp authentication pap
!
interface Virtual-Template2
ip unnumbered ATM0/0/0.9
ip route-cache cef
no ip directed-broadcast
peer default ip address pool pool-2
ppp authentication chap
!
vc-class atm pppoe
 encapsulation aal5autoppp Virtual-Template1
!
vc-class atm pppoa
 encapsulation aal5autoppp Virtual-Template2
!
```

Verifying PPP Autosense Configuration

To verify that you successfully configured PPPoA/PPPoE autosense, enter the **show running-config** EXEC command.

Monitoring and Maintaining PPPoA/PPPoE Autosense

Use the following commands to monitor and maintain PPPoA/PPPoE autosense:

Command	Purpose
`Router# show atm pvc [ppp]`	After the client at the other end of the PVC has initiated a PPPoA session, use this command to check that the PVC contains the PPPoA session.

Command	Purpose
`Router# show caller`	Enter this command to: • View individual users and consumed resources on the NAS. • Inspect active call statistics for large pools of connections. (The **debug** commands produce too much output and tax the CPU too heavily.) • Display the absolute and idle times for each user. The current values for both of these settings are displayed on the TTY line and the asynchronous interface. Users who have been idle for unacceptably long periods of time can be easily identified. By using this information, you can define timeout policies and multiple grades of services for different users.
`Router# show interface virtual access` *number*	Displays information about the virtual access interface, LCP, protocol states, and interface statistics. The status of the virtual access interface should read: `Virtual-Access3 is up, line protocol is up`

Troubleshooting PPPoA/PPPoE Autosense

To troubleshoot PPP sessions establishment, use the following commands:

- **debug ppp negotiation**
- **debug ppp authentication**

To troubleshoot the establishment of PPP sessions that are authenticated by a RADIUS or TACACS server, use the following commands:

- **debug aaa authentication**
- **debug aaa authorization**

Caution Use **debug** commands with extreme caution because they are CPU-intensive and can seriously impact your network.

PPPoE Session Count MIB

Note Before performing these tasks, read the Restrictions and Prerequisites sections.

The PPPoE Session-Count MIB provides the ability to use Simple Network Management Protocol (SNMP) to monitor in real time the number of PPPoE sessions configured on PVCs and on a router.

The PPPoE Session-Count MIB also introduces two SNMP traps that generate notification messages when a PPPoE session-count threshold is reached on any PVC or on the router. You can configure the PPPoE session-count thresholds by using the **pppoe limit max-sessions** and **pppoe max-sessions** commands.

Table 4-2 describes the objects and tables supported by the PPPoE Session-Count MIB. For a complete description of the MIB, see the PPPoE Sessions Management MIB file CISCO-PPPOE-MIB.my, available through Cisco.com at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Table 4-2 PPPoE Session Count MIB Objects and Tables

Object	Description
cPppoeSystemCurrSessions	Number of PPPoE sessions active on the router.
cPppoeSystemHighWaterSessions	Total number of PPPoE sessions configured on the router since the system was initialized.
cPppoeSystemMaxAllowedSessions	Number of PPPoE sessions configurable on the router.
cPppoeSystemThresholdSessions	Threshold value of PPPoE sessions configurable on the router.
cPppoeSystemExceededSessionErrors	Accumulated number of errors on the router that have occurred because the cPppoeSystemCurrSessions value exceeded the cPppoeSystemMaxAllowedSessions value.
cPppoeVcCfgTable	PPPoE protocol-related configuration information about the virtual channel links (VCLs).
cPppoeVcSessionsTable	Configuration information and statistics about the number of PPPoE sessions on the VCLs.
cPppoeSystemSessionThresholdTrap	Generates a notification message when the number of PPPoE sessions on the router reaches the configured threshold value.
cPppoeVcSessionThresholdTrap	Generates a notification message when the number of PPPoE sessions on the PVC reaches the configured threshold value.

The PPPoE Session Count MIB provides the following benefits:

- Allows the monitoring of PPPoE session counts using SNMP.
- Helps to manage the number of PPPoE sessions configured on a router or PVC by sending notification messages when the PPPoE session threshold has been reached.
- Provides a way to track PPPoE session information over time.

See the following sections for configuration tasks for the PPPoE Session Limit MIB feature. Each task in the list is identified as optional or required.

- Enabling PPPoE Session Count SNMP Traps (required)
- Configuring the PPPoE Session-Count Threshold for the Router (optional)
- Configuring the PPPoE Session-Count Threshold for a PVC (optional)
- Configuring the PPPoE Session Count Threshold for a VC Class (optional)
- Configuring the PPPoE Session-Count Threshold for an ATM PVC Range (optional)
- Configuring the PPPoE Session-Count Threshold for an Individual PVC Within a Range (optional)
- Verifying PPPoE Session Count Thresholds (optional)

Enabling PPPoE Session Count SNMP Traps

To enable SNMP traps that send notification messages when PPPoE session thresholds have been reached, use the following command in global configuration mode:

Command	Purpose
`Router(config)# snmp-server enable traps pppoe`	Enables PPPoE session-count Simple Network Management Protocol (SNMP) notifications.

Example: Enabling PPPoE Session-Count SNMP Traps

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
```

Configuring the PPPoE Session-Count Threshold for the Router

To configure the PPPoE session-count threshold for the router, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vpdn group` *name*	Associates a virtual private dialup network (VPDN) group with a customer or VPDN profile.
Step 2	`Router(config-vpdn)# accept dialin`	Creates an accept dial-in VPDN group.
Step 3	`Router(config-vpdn-acc-in)# protocol pppoe`	Configures the Layer 2 Tunneling Protocol (L2TP) that the VPDN subgroup will use.
Step 4	`Router(config-vpdn-acc-in)# virtual-template` *template-number*	Specifies the virtual template to clone virtual access interfaces.
Step 5	`Router(config-vpdn)# pppoe limit max-sessions` *number-of-sessions* [`threshold-sessions` *number-of-sessions*]	Sets the maximum number of PPPoE sessions that are permitted on a router, and sets the PPPoE session-count threshold at which an SNMP trap is generated.

Example: Configuring the PPPoE Session-Count Threshold for the Router

The following example shows a limit of 4000 PPPoE sessions configured for the router. The PPPoE session-count threshold is set at 3000 sessions, so when the number of PPPoE sessions on the router reaches 3000, an SNMP trap is generated.

```
vpdn enable
no vpdn logging
!
vpdn-group 1
 accept-dialin
  protocol pppoe
  virtual-template 1
```

```
pppoe limit max-sessions 4000 threshold-sessions 3000
```

Configuring the PPPoE Session-Count Threshold for a PVC

To configure the PPPoE session-count threshold for a PVC, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface atm number [point-to-point | multipoint]`	Configures an ATM interface.[1]
Step 2	`Router(config-if)# pvc [name] vpi/vci`	Configures the PVC.
Step 3	`Router(config-if-atm-vc)# pppoe max-session number-of-sessions [threshold-sessions number-of-sessions]`	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, virtual circuit (VC) class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap will be generated.

1. To determine the correct form of the **interface atm** command, consult your ATM network module, port adapter, or router documentation.

Example: Configuring the PPPoE Session-Count Threshold for a PVC

The following example shows a limit of 5 PPPoE sessions configured for the PVC. The PPPoE session-count threshold is set at 3 sessions, so when the number of PPPoE sessions on the PVC reaches 3, an SNMP trap is generated.

```
interface ATM0/0/0
 ip address 10.0.0.1 255.255.255.0
 no atm ilmi-keepalive
 pvc 5/120
  protocol ip 10.0.0.2 broadcast
  pppoe max-sessions 5 threshold-sessions 3
  protocol pppoe
```

Configuring the PPPoE Session Count Threshold for a VC Class

To configure the PPPoE session-count threshold for a VC class, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vc-class atm name`	Creates a VC class for an ATM PVC, SVC, or ATM interface.
Step 2	`Router(config-vc-class)# pppoe max-session number-of-sessions [threshold-sessions number-of-sessions]`	Sets the maximum number of PPPoE sessions that are permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap is generated.

Example: Configuring the PPPoE Session Count Threshold for a VC Class

The following example shows a limit of 7 PPPoE sessions configured for a VC class called “main”. The PPPoE session-count threshold is set at 3 sessions, so when the number of PPPoE sessions for the VC class reaches 3, an SNMP trap is generated.

```
vc-class atm main
 pppoe max-sessions 7 threshold-sessions 3
```

Configuring the PPPoE Session-Count Threshold for an ATM PVC Range

To configure the PPPoE session- count threshold for an ATM PVC range, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface atm number [point-to-point | multipoint]`	Configures an ATM interface.[1]
Step 2	`Router(config-if)# range [range-name] pvc start-vpi/start-vci end-vpi/end-vci`	Defines a range of ATM PVCs.
Step 3	`Router(cfg-if-atm-range)# pppoe max-session number-of-sessions [threshold-sessions number-of-sessions]`	Sets the maximum number of PPPoE sessions that are permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap is generated.

1. To determine the correct form of the **interface atm** command, consult your ATM network module, port adapter, or router documentation.

Example: Configuring the PPPoE Session-Count Threshold for an ATM PVC Range

The following example shows a limit of 20 PPPoE sessions configured for the PVC range. The PPPoE session-count threshold is also be 20 sessions because when the session-count threshold has not been explicitly configured, it defaults to the PPPoE session limit. An SNMP trap is generated when the number of PPPoE sessions for the range reaches 20.

```
interface ATM0/0/0.3 point-to-point
 range pvc 3/100 3/105
  pppoe max-sessions 20
  protocol pppoe
```

Configuring the PPPoE Session-Count Threshold for an Individual PVC Within a Range

To configure the PPPoE session-count threshold for an individual PVC within an ATM PVC range, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface atm number [point-to-point | multipoint]`	Configures an ATM interface.[1]
Step 2	`Router(config-if)# range [range-name] pvc start-vpi/start-vci end-vpi/end-vci`	Defines a range of ATM PVCs.

	Command	Purpose
Step 3	`Router(cfg-if-atm-range)# pvc-in-range [pvc-name] [vpi/vci]`	Configures an individual PVC within a PVC range.
Step 4	`Router(cfg-if-atm-range-pvc)# pppoe max-session number-of-sessions [threshold-sessions number-of-sessions]`	Sets the maximum number of PPPoE sessions that are permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session-count threshold at which an SNMP trap is generated.

1. To determine the correct form of the **interface atm** command, consult your ATM network module, port adapter, or router documentation.

Example: Configuring the PPPoE Session-Count Threshold for an Individual PVC Within a Range

The following example shows a limit of 10 PPPoE sessions configured for "pvc1". The PPPoE session-count threshold is set at 3 sessions, so when the number of PPPoE sessions for the PVC reaches 3, an SNMP trap is generated.

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

Verifying PPPoE Session Count Thresholds

To verify the configuration of PPPoE session-count thresholds, use the following command in EXEC mode:

Command	Purpose
`Router# more system:running-config`	Displays the running configuration.

Monitoring and Maintaining PPPoE Session Counts and SNMP Notifications

To monitor PPPoE session counts and SNMP notifications, use the following commands in EXEC mode:

Command	Purpose
`Router# debug snmp packets`	Displays information about every SNMP packet sent or received by the router.
`Router# 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.
`Router# debug vpdn pppoe-packets`	Displays each PPPoE protocol packet exchanged.
`Router# show vpdn [session][packets][tunnel][all]`	Displays information about active tunnel and message identifiers in a VPDN.

CHAPTER 5

Session and Tunnel Scalability

This chapter describes parameters that you can modify to optimize the session and tunnel scalability on the Cisco 6400 in Cisco IOS Release 12.2(4)B.

Note For supported scalability numbers and the recommended parameter values for achieving those numbers, see the "Important Notes" section of the Cisco 6400 Release Notes.

This chapter includes the following sections:

Recommendations

Memory

See the Cisco 6400 Release Notes for memory recommendations.

Image Versions

Make sure that the NSP and NRP simultaneously run the same software release version.

System and Console Logging

Disable logging to the console terminal by using the **no logging console** global configuration command:

```
Router(config)# no logging console
```

Also, log messages to an internal buffer by using the **logging buffered** *buffer-size* global configuration command. Choose a buffer size appropriate for the available memory and volume of messages logged on your systems:

```
Router(config)# logging buffered 131072
```

For more information on system and console logging, see the "Redirecting debug and error message Output" section of the "Using Debug Commands" chapter of the *Cisco IOS Debug Command Reference*.

Restrictions

Precloning

For the NRP-1 using 128 MB of DRAM, the total number of precloned interfaces must not exceed 3000.

IP QoS

Downloading policing parameters from a AAA server might reduce the number of PPP sessions that can be established per second. See the Cisco 6400 Release Notes for details.

Input and Output Hold-Queues

The input and output hold-queue limits determine the maximum number of incoming and outgoing control packets that the queue can accommodate. The default input and output hold-queue limits depend on the NRP type (see Table 5-1).

Table 5-1 Default Input and Output Hold-Queue Limits

NRP Type	Default Input Hold-Queue Limit	Default Output Hold-Queue Limit
NRP-1	75 packets	80 packets
NRP-2	75 packets	40 packets

Tip If you enter the **show interfaces** EXEC command and see an excessive number of discarded packets due to input or output hold-queue overflows, then increase the appropriate hold-queue limit.

Configuring the Input or Output Hold-Queue Limit

To modify the input or output hold-queue limit, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface atm 0/0/0`	Selects the ATM interface.
Step 2	`Router(config-if)# hold-queue` *length* {**in** | **out**}	Specifies the maximum number of packets in the input or output hold-queue. See Table 5-1 for default values.

Verifying the Input and Hold-Queue Limits

To display the current hold-queue limits and the number of packets discarded because of hold-queue overflows, use the **show interface atm 0/0/0** EXEC command.

Example: Verifying the Input and Output Hold-Queue Limits

In the following example, the NRP-2 input and output hold-queue limits are set to 4096 packets:

```
Router# show interface atm 0/0/0
ATM0/0/0 is up, line protocol is up
  Hardware is NRP2 ATM SAR
  MTU 1900 bytes, sub MTU 1900, BW 599040 Kbit, DLY 60 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not supported
  Keepalive not supported
  Encapsulation(s):AAL5
  16384 maximum active VCs, 2048 VCs per VP, 4002 current VCCs
  VC idle disconnect time:300 seconds
  0 carrier transitions
  Last input never, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy:fifo
➔ Output queue 0/4096, 0 drops; input queue 0/4096, 0 drops
  30 second input rate 29000 bits/sec, 213 packets/sec
  30 second output rate 28000 bits/sec, 253 packets/sec
     35846 packets input, 672141 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     81291 packets output, 1110355 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
Router#
```

LCP Session Initiations

The first phase of PPP, Link Control Protocol (LCP), is responsible for establishing, configuring, testing, maintaining, and terminating the PPP data-link connection. By default, the NRP does not limit the number of simultaneous LCP session initiations. When a large number of PPP sessions start at the same time (due to an NRP reload or an ATM interface reset), the numerous LCP requests can cause a spike in the CPU utilization. If the CPU is unable to service all the LCP requests simultaneously, LCP sessions

begin to timeout and renegotiate. This can result in a chain reaction of LCP session negotiations and excessive session recovery times. The chain reaction can be controlled by limiting the number of simultaneous LCP session initiations.

Limiting the Number of Simultaneous LCP Session Initiations

Note Only follow this procedure if the NRP has problems recovering after a reload or link dropout.

To limit the number of simultaneous LCP session initiations, enter the following commands in global configuration mode:

Command	Purpose
`Router(config)# lcp max-session-starts` *number*	Specifies the maximum number of simultaneous LCP sessions to be negotiated. Value must be between 100 and 3000 sessions.
`Router(config)# lcp max-load-metric` *number*	Specifies the maximum load metric, which determines the PPP manager process input queue length beyond which the NRP stops accepting new PPP LCP sessions.

Note The nominal values depend on many factors. Check the “Important Notes” section of the Cisco 6400 Release Notes for recommended values to use as a starting point. Try several numbers and select the combination that results in the shortest session recovery time after a link dropout.

Verifying the Simultaneous LCP Session Initiation Limit

To check the configured load metric and LCP session initiation limits, use the **show running-config** EXEC command.

PPP Timeouts

The PPP authentication timeout determines how long the system waits for a response from the remote peer before retransmitting one of the following packets:

- Password Authentication Protocol (PAP) authentication request
- Challenge Handshake Authentication Protocol (CHAP) challenge
- CHAP response

The PPP retry timeout determines how long the PPP state machine (for LCP and all NCP's) waits for a response from the remote peer before retransmitting one of the following packets:

- Configuration request
- Connection termination request

The default PPP authentication timeout is 10 seconds, and the default PPP retry timeout is 2 seconds. By modifying these values, you can help to optimize the number of stable PPP sessions.

Configuring the PPP Timeouts

To modify the PPP timeouts, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface virtual-template` *number*	Selects or creates the virtual template interface and enters interface configuration mode.
Step 2	`Router(config-if)# ppp timeout authentication` *seconds*	0 - 255. Specifies the PPP authentication timeout, in seconds. Default is 10 seconds.
Step 3	`Router(config-if)# ppp timeout retry` *seconds*	1 - 255. Specifies the PPP retry timeout, in seconds. Default is 2 seconds.

Note The nominal value depends on many factors. Check the "Important Notes" section of the Cisco 6400 Release Notes for recommended values to use as a starting point. Try several values and select the combination that results in the highest number of stable sessions.

Verifying the PPP Timeouts

To check the configured PPP authentication and retry timeouts, use the **show running-config** EXEC command.

Keepalives

You can configure the keepalive interval, which is the frequency at which the Cisco IOS software sends messages to ensure that a network interface or L2TP tunnel is alive. By default, the interface keepalive is 10 seconds, and the L2TP tunnel keepalive is 60 seconds. An interface is declared down after the fourth successive keepalive is sent without an echo reply.

The L2TP tunnel keepalive timers do not have to use the same value on both sides of the tunnel. For example, a LAC can use a keepalive value of 30 seconds, and an LNS can use the default value of 60 seconds.

A high interface keepalive interval is required when scaling up your session count. As rough examples, a value around 120 seconds may be best for an NRP-1 with 2000 sessions, while 200 seconds may be best for an NRP-2 with 8000 sessions. See the Cisco 6400 Release Notes for specific recommended values.

Keepalive interval configuration consists of the following tasks:

- Configuring the Interface Keepalive Interval
- Configuring the L2TP Tunnel Keepalive Interval

Configuring the Interface Keepalive Interval

To configure the interface keepalive interval, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface virtual-template number`	Selects or creates the virtual template interface and enters interface configuration mode.
Step 2	`Router(config-if)# keepalive [seconds]`	Sets the keepalive timer. Default is 10 seconds.

Verifying the Interface Keepalive Interval

To verify the interface keepalive interval, use the **show interface virtual-template** EXEC command.

Example: Verifying the Interface Keepalive Interval

In the following example, the interface keepalive interval is set to 200 seconds:

```
Router# show interface virtual-template 1
Virtual-Template1 is down, line protocol is down
  Hardware is Virtual Template interface
  Interface is unnumbered. Using address of GigabitEthernet0/0/0 (10.24.24.1)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, loopback not set
  Keepalive set (200 sec)
  DTR is pulsed for 5 seconds on reset
  LCP Closed
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 02:11:27
  Queueing strategy:fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
Router#
```

Configuring the L2TP Tunnel Keepalive Interval

To configure the L2TP tunnel keepalive interval, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vpdn-group number`	Selects the VPDN group.
Step 2	`Router(config-vpdn)# l2tp tunnel hello hello-interval`	The interval, in seconds, that the LAC and LNS wait before sending the next L2TP tunnel keepalive packet. Default is 60 seconds.

Verifying the L2TP Tunnel Keepalive Interval

To verify the L2TP tunnel keepalive interval, use the **show running-config** EXEC command.

Virtual Access Interface Precloning

Precloning (or allocating) virtual access interfaces when you start the system reduces the load on the system during call setup. Precloning is required to optimize scalability on:

- Network access server (NAS)—PPPoE terminated
- LAC and LNS—PPPoE/L2TP
- LNS—PPPoA/L2TP

Note Do not use precloning with PPPoA terminated.

Note The precloning operation might take a long time to complete (on the order of minutes for a large number of interfaces). Avoid incoming calls at the LNS until precloning is finished. You can monitor the precloning operation with the **show vtemplate** privileged EXEC command.

Precloning Virtual Access Interfaces

To preclone a virtual access interface, enter the following command in global configuration mode.

Command	Purpose
`Router(config)# virtual-template template-number pre-clone number`	Specifies the number of virtual access interfaces to be created and cloned from a specific virtual template.

Verifying the Precloned Virtual Access Interfaces

To check the successful precloning of virtual access interfaces, enter the privileged EXEC command **show vtemplate**. 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
```

L2TP Control Channel Parameters

By default, the NRP attempts 10 L2TP control channel retransmissions that follow an exponential backoff (such as 1, 2, 4, 8, 8, 8 seconds), starting at the minimum retransmission timeout (1 second by default), and ending at the maximum retransmission timeout (8 seconds by default).

To determine the best minimum and maximum retransmission timeouts for a given topology, enter the privileged EXEC command **show vpdn tunnel all**. Check the displayed retransmit time distribution:

```
Retransmit time distribution: 0 0 0 0 1 0 0 0 1
```

Each value corresponds to the number of retransmissions at 0, 1, 2,..., 8 seconds, respectively, displaying a histogram of all tunnel retransmission times.

The local control channel receive window size (RWS) determines how many incoming control messages can be acknowledged and waiting on the recipient's queue, instead of waiting on the peer's queue. Large values enable the NRP to open PPP sessions more quickly. The default local RWS is 3000 packets, which allows the L2TP control channel to send requests as fast as possible.

By improving L2TP control channel processing, the following tasks can provide resilience to dropouts between the LAC and the LNS:

- Configuring the Control Channel Retransmission Parameters
- Configuring the Local Control Channel Receive Window Size

Configuring the Control Channel Retransmission Parameters

To configure the L2TP control channel retransmission parameters, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vpdn-group` *number*	Selects the VPDN group.
Step 2	`Router(config-vpdn)# l2tp tunnel retransmit retries` *value*	Specifies the number of control channel retransmission attempts. Default is 10 retries.

	Command	Purpose
Step 3	`Router(config-vpdn)# l2tp tunnel retransmit timeout min seconds`	Specifies the minimum timeout for control channel retransmissions. Default is 1 second.
Step 4	`Router(config-vpdn)# l2tp tunnel retransmit timeout max seconds`	Specifies the maximum timeout (up to 8 seconds) for control channel retransmissions. Default is 8 seconds.

Verifying the Control Channel Retransmission Parameters

To check the configured L2TP control channel retransmission parameters, enter the **show running-config** EXEC command.

To check general control channel retransmission parameters, enter the **show vpdn tunnel all** privileged EXEC command.

Configuring the Local Control Channel Receive Window Size

To configure the local control channel RWS, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# vpdn-group number`	Selects the VPDN group.
Step 2	`Router(config-vpdn)# l2tp tunnel receive-window packets`	Specifies the size of advertised receive window. Default is 3000 packets.
Step 3	`Router(config-vpdn)# exit`	Returns to global configuration mode.
Step 4	`Router(config)# end`	Returns to privileged EXEC mode.
Step 5	`Router# clear vpdn tunnel l2tp remote-name local-name`	Clears all sessions and drops the tunnel.

Verifying the Local Control Channel Receive Window Size

To display the local control channel RWS, use the **show vpdn tunnel all** privileged EXEC command.

```
Router# show vpdn tunnel all

 L2TP Tunnel Information (Total tunnels=1 sessions=500)

 Tunnel id 20 is up, remote id is 12, 500 active sessions
   Tunnel state is established, time since change 00:00:33
   Remote tunnel name is LAC
     Internet Address 10.1.1.1, port 1701
   Local tunnel name is LNS
     Internet Address 10.1.1.2, port 1701
   971 packets sent, 1259 received, 19892 bytes sent, 37787 received
   Control Ns 501, Nr 746
➔  Local RWS 3000 (default), Remote RWS 3000 (max)
   Retransmission time 4, max 8 seconds
   Unsent queuesize 0, max 0
   Resend queuesize 251, max 261
```

```
Total resends 390, ZLB ACKs 251
Current nosession queue check 0 of 5
Retransmit time distribution: 0 0 0 0 1 0 0 0 1
Sessions disconnected due to lack of resources 0
```

L2TP Tunnel Timeout

The tunnel timeout determines how long a tunnel lingers after all its sessions are gone. The default tunnel timeout is 10 seconds for an LNS and 15 seconds for a LAC. Configuring a longer tunnel timeout is useful:

- After all the tunnel sessions are gone and you expect sessions to come back immediately.
- If you plan to examine the tunnel status after the sessions have ended.

Configuring the L2TP Tunnel Timeout

To configure the L2TP tunnel timeout, enter the following commands beginning in global configuration mode.

	Command	Purpose
Step 1	`Router(config)# vpdn-group number`	Selects the VPDN group.
Step 2	`Router(config-vpdn)# l2tp tunnel nosession-timeout seconds`	Specifies the tunnel timeout length. LNS default is 10 seconds, and LAC default is 15 seconds.

Verifying the L2TP Tunnel Timeout

To check the configured tunnel timeout, use the **show running-config** EXEC command.

An Example Configuration of Session and Tunnel Scalability Parameters

For general L2TP configuration examples, see the *Layer 2 Tunnel Protocol* feature module and the "Configuring Virtual Private Networks" chapter in the "Virtual Templates, Profiles, and Networks" part of the *Cisco IOS Dial Technologies Configuration Guide*.

The following example shows a configuration implementing the session and tunnel scalability optimization commands described in this chapter.The input hold queue limit on an ATM interface is set to 1200, and virtual template 1 is used to preclone 2000 virtual access interfaces. VPDN group 1 is set to use 7 retransmission attempts, with the retransmission timeouts beginning at 2 seconds and ending at 4 seconds. The L2TP tunnel timeout is set to 10 seconds. The local RWS is set to 500 packets. The number of simultaneous LCP session initiations are limited to 100, and the load metric is limited to 100. Both the PPP authentication and retry timeouts are set to 15 seconds.

```
!
vpdn enable
!
```

```
vpdn-group 1
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate from hostname LAC1
 local name LNS1
 l2tp tunnel receive-window 500
 l2tp tunnel nosession-timeout 10
 l2tp tunnel retransmit retries 7
 l2tp tunnel retransmit timeout min 2
 l2tp tunnel retransmit timeout max 4
!
!
virtual-template 1 pre-clone 2000
!
interface ATM 0/0/0
 hold-queue 1200 in
!
interface FastEthernet 0/0/0
 ip address negotiated
 no ip directed-broadcast
!
interface Virtual-Template 1
 ip unnumbered FastEthernet 0/0/0
 no ip directed-broadcast
 no logging event link-status
 no keepalive
 peer default ip address pool pool-1
 ppp authentication chap
 ppp timeout retry 15
 ppp timeout authentication 15
!
lcp max-session-starts 100
lcp max-load-metric 100
!
```

Monitoring and Maintaining PPP Scalability

Use the following commands to monitor and maintaining PPP scalability:

Command	Purpose
Router# **show atm pvc ppp**	(PPPoA and PPPoE) Displays each PVC configured for PPP.
Router# **show ip local pool**	(PPPoA and PPPoE) Displays the local address pools.
Router# **show vpdn tunnel** [**all** | **packets** | **state** | **summary** | **transport**] [**id** | **local-name** | **remote-name**]	(PPPoE only) Displays VPDN tunnel information including tunnel protocol, ID, packets sent and received, receive window sizes, retransmission times, and transport status.
Router> **clear vpdn tunnel l2tp** *remote-name local-name*	(PPPoE only) Shuts down a specific tunnel and all the sessions within the tunnel.

Examples

```
Router# show atm pvc ppp
           VCD /                                          Peak  Avg/Min Burst
ATM Int.   Name          VPI   VCI  Type   VA VASt  SC   Kbps   Kbps   Cells VCSt
0/0/0.101  2               1    41  PVC     1 DOWN UBR  599040                UP
0/0/0.101  3               1    42  PVC     2 DOWN UBR  599040                UP
0/0/0.101  4               1    43  PVC     3 DOWN UBR  599040                UP
0/0/0.101  5               1    44  PVC     4 DOWN UBR  599040                UP
0/0/0.101  6               1    45  PVC     5 DOWN UBR  599040                UP
0/0/0.101  7               1    46  PVC     6 DOWN UBR  599040                UP
0/0/0.101  8               1    47  PVC     7 DOWN UBR  599040                UP
0/0/0.101  9               1    48  PVC     8 DOWN UBR  599040                UP
0/0/0.101  10              1    49  PVC     9 DOWN UBR  599040                UP
0/0/0.101  11              1    50  PVC    10 DOWN UBR  599040                UP
0/0/0.101  12              1    51  PVC    11 DOWN UBR  599040                UP
0/0/0.101  13              1    52  PVC    12 DOWN UBR  599040                UP
0/0/0.101  14              1    53  PVC    13 DOWN UBR  599040                UP

Router# show ip local pool

 Pool                    Begin           End             Free  In use
 pool1                   110.1.1.1       110.1.1.250       10     240
                         110.1.2.1       110.1.2.250        3     247
                         110.1.3.1       110.1.3.250        1     249
                         110.1.4.1       110.1.4.250        6     244
                         110.1.5.1       110.1.5.250        1     249
                         110.1.6.1       110.1.6.250        4     246
                         110.1.7.1       110.1.7.250        2     248
                         110.1.8.1       110.1.8.250        2     248
                         110.1.9.1       110.1.9.250        3     247
                         110.1.10.1      110.1.10.250       3     247
                         110.1.11.1      110.1.11.250       3     247
                         110.1.12.1      110.1.12.250       7     243
                         110.1.13.1      110.1.13.250       2     248
```

Monitoring and Maintaining L2TP Scalability

For general information on monitoring and maintaining L2TP, see the *Layer 2 Tunnel Protocol* feature module and the "Configuring Virtual Private Networks" chapter in the "Virtual Templates, Profiles, and Networks" part of the *Cisco IOS Dial Technologies Configuration Guide*.

Use the following commands to monitor and maintain L2TP scalability:

Command	Purpose
Router# **show vpdn tunnel** [**all** | **packets** | **state** | **summary** | **transport**] [**id** | **local-name** | **remote-name**]	Displays VPDN tunnel information including tunnel protocol, ID, packets sent and received, receive window sizes, retransmission times, and transport status.
Router# **show vpdn session** [**all** [**interface** | **tunnel** | **username**]| **packets** | **sequence** | **state** | **timers** | **window**]	Displays VPDN session information including interface, tunnel, username, packets, status, and window statistics.
Router> **clear vpdn tunnel l2tp** *remote-name local-name*	Shuts down a specific tunnel and all the sessions within the tunnel.

The **show vpdn tunnel all** privileged EXEC command output includes scalability parameters. Scalability-related fields are described in Table 5-2.

```
Router# show vpdn tunnel all

 L2TP Tunnel Information (Total tunnels=1 sessions=500)

 Tunnel id 20 is up, remote id is 12, 500 active sessions
   Tunnel state is established, time since change 00:00:33
   Remote tunnel name is LAC
     Internet Address 10.1.1.1, port 1701
   Local tunnel name is LNS
     Internet Address 10.1.1.2, port 1701
   971 packets sent, 1259 received, 19892 bytes sent, 37787 received
   Control Ns 501, Nr 746
   Local RWS 3000 (default), Remote RWS 3000 (max)
   Retransmission time 4, max 8 seconds
   Unsent queuesize 0, max 0
   Resend queuesize 251, max 261
   Total resends 390, ZLB ACKs 251
   Current nosession queue check 0 of 5
   Retransmit time distribution: 0 0 0 0 1 0 0 0 1
   Sessions disconnected due to lack of resources 0
```

Table 5-2 Scalability-Related* show vpdn tunnel all *Field Descriptions

Field (as it appears in previous example)	Description
Retransmission time 4, max 8 seconds	Current retransmit timeout for the tunnel; maximum retransmit timeout reached by the tunnel.
Unsent queuesize 0, max 0	Number of control packets waiting to be sent to the peer; maximum number of control packets in the unsent queue.
Resend queuesize 251, max 261	Number of control packets sent but not acknowledged; maximum number of unacknowledged control packets in the resend queue.
Total resends 390, ZLB ACKs 251	Total number of packets resent; number of zero length body acknowledgment messages sent.
Current nosession queue check 0 of 5	Number of tunnel timeout periods since the last session ended. Up to 5 tunnel timeouts are used if there are outstanding control packets on the unsent or resend queue. Otherwise, the tunnel is dropped after 1 tunnel timeout.
Retransmit time distribution: 0 0 0 0 1 0 0 0 1	Histogram showing the number of retransmissions at 0, 1, 2,..., 8 seconds, respectively.
Sessions disconnected due to lack of resources 0	Number of sessions for which there were no precloned interfaces available. By default, a request for a new session at an LNS is refused if a precloned interface is not available.

CHAPTER 6

Miscellaneous Features

This chapter describes the following features:

Routing and Bridging

The following common routing and bridging protocols are detailed in the examples in this section:

- Standard bridging (using RFC 1483 encapsulation)
- Subscriber bridging
- Integrated routing and bridging (IRB)
- Standard routing (using RFC 1483 encapsulation)

For more information about routing and bridging, refer to the Cisco IOS *Network Protocols Configuration Guide, Part 1* and the *Bridging and IBM Networking Configuration Guide.*

The Cisco 6400 NRP also offers routed bridging, which encapsulates bridged traffic in RFC 1483 routed packets. ATM routed bridging takes advantage of the characteristics of a stub LAN topology commonly used for digital subscriber line (DSL) access. For more information, see the "Configuring Broadband Access: PPP and Routed Bridge Encapsulation" chapter of the *Cisco IOS Wide-Area Networking Configuration Guide*.

Configuring an Interface or Subinterface for Routing or Bridging

To configure an interface or subinterface for routing or bridging, perform the following tasks starting in global configuration mode:

	Command	Purpose
Step 1	**interface atm 0/0/0** [*.subinterface-number* {**multipoint** | **point-to-point**}]	Specifies the ATM interface and optional subinterface.
Step 2	**pvc** [*name*] *vpi/vci*	Configures a new ATM PVC by assigning a name (optional) and VPI/VCI numbers.
Step 3	encapsulation aal5snap[1]	Configures AAL5 with SNAP encapsulation.
Step 4	**protocol** *protocol* [*protocol-address* | **inarp**] [[**no**] **broadcast**]	Maps a protocol address to the PVC.

1. AAL5 with SNAP encapsulation is defined by default for all PVCs. This command must be used to override a different encapsulation type at the interface or subinterface level.

Example—Configuring RFC 1483 Bridging on a Multipoint Interface

The following example shows how to configure RFC 1483 bridging on a multipoint interface. Arrows indicate subscriber bridging steps:

```
Router(config)# interface atm 0/0/0.10 multipoint
Router(config-if)# no ip address
Router(config-if)# bridge-group 1

Router(config-if)# pvc 1 32
Router(config-if-atm-vc)# encapsulation aal5snap
Router(config-if-atm-vc)# protocol bridge broadcast
Router(config-if-atm-vc)# exit

Router(config-if)# pvc 1 33
Router(config-if-atm-vc)# encapsulation aal5snap
Router(config-if-atm-vc)# protocol bridge broadcast
Router(config-if-atm-vc)# exit
Router(config-if)# exit

Router(config)# bridge 1 protocol ieee
➔ Router(config)# bridge 1 subscriber-policy 5
➔ Router(config)# subscriber-policy 5 no ipx permit
```

Example—Configuring RFC1483 Bridging on a Point-to-Point Interface

The following example shows how to configure RFC1483 bridging on a point-to-point interface. Arrows indicate integrated routing and bridging steps:

```
Router(config)# interface atm 0/0/0.20 point-to-point
Router(config-if)# no ip address
Router(config-if)# bridge-group 2
Router(config-if)# pvc 2 32
Router(config-if-atm-vc)# encapsulation aal5snap
Router(config-if-atm-vc)# protocol bridge broadcast
Router(config-if-atm-vc)# exit
Router(config-if)# exit

Router(config)# interface atm 0/0/0.21 point-to-point
```

```
Router(config-if)# no ip address
Router(config-if)# bridge-group 2
Router(config-if)# pvc 2 33
Router(config-if-atm-vc)# encapsulation aal5snap
Router(config-if-atm-vc)# protocol bridge broadcast
Router(config-if-atm-vc)# exit
Router(config-if)# exit

Router(config)# bridge irb
Router(config)# interface bvi 2
Router(config-if)# ip address 172.26.13.49
Router(config-if)# exit

Router(config)# bridge 2 protocol ieee
Router(config)# bridge 2 route ip
Router(config)# bridge 2 bridge ipx
```

Example—Configuring RFC 1483 IP Routing

The following example shows how to configure RFC 1483 IP routing. When configuring IP on a PVC, you must either enable inverse ARP (InARP) or enter a static map:

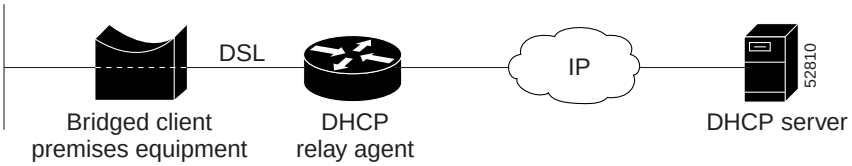
```
Router(config)# interface atm 0/0/0.40 multipoint
Router(config-if)# ip address 172.25.210.97 255.255.0.0

Router(config-if)# pvc 4 32
Router(config-if-atm-vc)# encapsulation aal5snap
Router(config-if-atm-vc)# protocol ip inarp broadcast
Router(config-if-atm-vc)# exit

Router(config-if)# pvc 4 33
Router(config-if-atm-vc)# encapsulation aal5snap
Router(config-if-atm-vc)# protocol ip 10.3.45.156 broadcast
Router(config-if-atm-vc)# exit
Router(config-if)# exit

Router(config)# interface atm 0/0/0.41 point-to-point
Router(config-if)# ip unnumbered fastethernet 0/0/0

Router(config-if)# pvc 4 34
Router(config-if-atm-vc)# encapsulation aal5snap
Router(config-if-atm-vc)# protocol ip inarp broadcast
Router(config-if-atm-vc)# exit
Router(config-if)# exit
```

DHCP Option 82 Support for Routed Bridge Encapsulation

The DHCP relay agent information option (option 82) enables a Dynamic Host Configuration Protocol (DHCP) relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement IP address or other parameter-assignment policies.

The DHCP Option 82 Support for Routed Bridge Encapsulation feature provides support for the DHCP relay agent information option when ATM routed bridge encapsulation (RBE) is used. Figure 6-1 shows a typical network topology in which ATM RBE and DHCP are used. The aggregation router that is using ATM RBE is also serving as the DHCP relay agent.

Figure 6-1 Network Topology Using ATM RBE and DHCP



This feature communicates information to the DHCP server by using a suboption of the DHCP relay agent information option called *agent remote ID*. The information that is sent in the agent remote ID includes an IP address identifying the relay agent and information about the ATM interface and the PVC over which the DHCP request came in. The DHCP server can use this information to make IP address assignments and security policy decisions.

Note For the Cisco 6400 as the DHCP relay agent, the IP address used in the agent remote ID is always the network management Ethernet (NME) interface of the NSP.

Figure 6-2 shows the format of the agent remote ID suboption.

Figure 6-2 Format of the Agent Remote ID Suboption

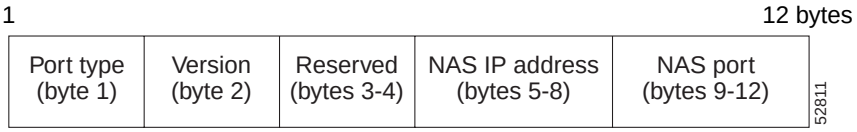


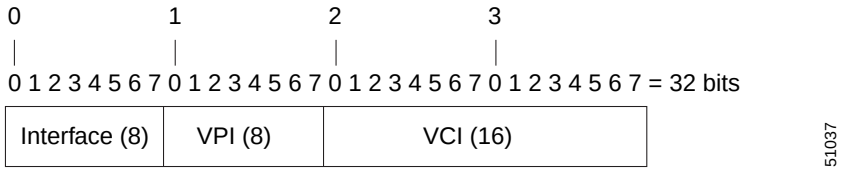
Table 6-1 describes the agent remote ID suboption fields displayed in Figure 6-2.

Table 6-1 Agent Remote ID Suboption Field Descriptions

Field	Description
Port Type	Port type. The value 0x01 indicates RBE (1 byte).
Version	Option 82 version. The value 0x01 specifies the RBE version of Option 82 (1 byte).
Reserved	Reserved (2 bytes).
NAS IP Address	IP address of the NSP NME interface.
NAS Port	RBE-enabled virtual circuit on which the DHCP request has come in. See Figure 6-3 for the format of this field (4 bytes).

Figure 6-3 shows the format of the network access server (NAS) port field in the agent remote ID suboption.

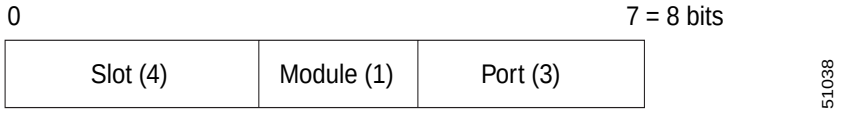
Figure 6-3 Format of the NAS Port Field



Note For soft PVCs, the NAS port field contains the *egress* VPI/VCI values. Otherwise, the ingress VPI/VCI values are used.

Figure 6-4 shows the format of the interface field. If there is no module, the value of the module bit is 0.

Figure 6-4 Format of the Interface Field



Note For soft PVCs, the interface field uses the *egress* slot/subslot/port information.

Benefits

Service providers are increasingly using ATM routed bridge encapsulation to configure digital subscriber line (DSL) access. The DHCP Option 82 Support for Routed Bridge Encapsulation feature enables those service providers to use DHCP to assign IP addresses and DHCP option 82 to implement security and IP address assignment policies.

Related Documents

- *Cisco IOS IP Configuration Guide*
- *Cisco IOS IP Command Reference*
- *Cisco IOS Wide-Area Networking Configuration Guide*
- *Cisco IOS Wide-Area Networking Command Reference*

Configuring DHCP Option 82 for RBE

To configure DHCP option 82 support for RBE, use the following command in global configuration mode:

Command	Purpose
`Router(config)# ip dhcp relay information option`	Enables the system to insert the DHCP relay agent information option in forwarded BOOT REQUEST messages to a Cisco IOS DHCP server.

Verifying DHCP Option 82 for RBE Configuration

To verify that the DHCP Option 82 Support for Routed Bridge Encapsulation feature is configured correctly, use the following command in privileged EXEC mode:

Command	Purpose
`Router# more system:running-config`	Displays the running configuration.

Example—DHCP Option 82 for RBE With Soft PVC

In the following example, DHCP option 82 support is enabled on a DHCP relay agent that uses a soft PVC to connect to the DSLAM:

```
ip dhcp relay information option
!
interface Loopback0
 ip address 10.40.40.1 255.255.255.0
!
interface Loopback1
 ip address 10.40.50.1 255.255.255.0
!

interface ATM0/0/0
 no ip address
 no atm ilmi-keepalive
 hold-queue 1000 in
!
interface ATM0/0/0.3 point-to-point
 ip unnumbered Loopback0
 ip helper-address 10.60.60.2
 atm route-bridged ip
 pvc 1/50
  encapsulation aal5snap
 !
!
interface FastEthernet0/0/0
 ip address 10.60.60.1 255.255.255.0
 no keepalive
 full-duplex
!
router rip
 network 10.0.0.0
!
```

In this configuration example, the value (in hexadecimal) of the agent remote ID suboption would be 010100009c13233940010032. Table 6-2 shows the value of each field within the agent remote ID suboption.

Table 6-2 Agent Remote ID Suboption Field Descriptions—Soft PVC

Agent Remote ID Suboption Field	Value
Port Type	0x01
Version	0x01
Reserved	undefined
NAS IP Address	0x9c132339 (hexadecimal value of 172.19.35.57)
NAS Port • Interface (slot/module/port) • VPI • VCI	egress port information[1] • 0x40 (The slot/module/port values are 4/0/0) • 0x01 (hexadecimal value of 1) • 0x32 (hexadecimal value of 50)

1. Because a soft PVC connects the DHCP relay agent to the DSLAM, the NAS port field uses the *egress* port information.

Example—DHCP Option 82 for RBE With PVC

In the following example, DHCP option 82 support is enabled on a DHCP relay agent that uses a PVC to connect to the DSLAM:

```
ip dhcp relay information option
!
interface Loopback0
 ip address 10.40.40.1 255.255.255.0
!
interface Loopback1
 ip address 10.40.50.1 255.255.255.0
!

interface ATM0/0/0
 no ip address
 no atm ilmi-keepalive
 hold-queue 1000 in
!
interface ATM0/0/0.4 point-to-point
 ip unnumbered Loopback0
 ip helper-address 10.60.60.2
 atm route-bridged ip
 pvc 1/51
  encapsulation aal5snap
 !
!
interface FastEthernet0/0/0
 ip address 10.60.60.1 255.255.255.0
 no keepalive
 full-duplex
!
router rip
 network 10.0.0.0
!
```

In this configuration example, the value (in hexadecimal) of the agent remote ID suboption would be 010100009c13233970010035. Table 6-3 shows the value of each field within the agent remote ID suboption.

Table 6-3 Agent Remote ID Suboption Field Descriptions —PVC

Agent Remote ID Suboption Field	Value
Port Type	0x01
Version	0x01
Reserved	undefined
NAS IP Address	0x9c132339 (hexadecimal value of 172.19.35.57)
NAS Port	ingress port information[1]
• Interface (slot/module/port)	• 0x70 (The slot/module/port values are 7/0/0)
• VPI	• 0x01 (hexadecimal value of 1)
• VCI	• 0x35 (hexadecimal value of 53)

1. Because a PVC connects the DHCP relay agent to the DSLAM, the NAS port field uses the *ingress* port information.

RADIUS VC Logging

RADIUS virtual circuit (VC) logging allows the Cisco 6400 to accurately record the virtual path interface (VPI) and virtual circuit interface (VCI) of an incoming subscriber session.

Note For soft PVCs, the Cisco 6400 returns the *egress* slot/subslot/port and VPI/VCI information.

With RADIUS VC logging enabled, the RADIUS network access server (NAS) port field is extended and modified to carry VPI/VCI information. This information is logged in the RADIUS accounting record that was created at session startup.

To display the VPI/VCI information that can be used by the RADIUS VC Logging feature, use the **show atm ingress** command in EXEC mode.

RADIUS VC Logging feature configuration consists of these tasks:

- Task 1: Configuring the NME Interface IP Address on the NSP
- Task 2: Configuring RADIUS VC Logging on the NRP
- Task 3: Selecting the IP Address for RADIUS Attribute 4 (NAS-IP Address)

Task 1: Configuring the NME Interface IP Address on the NSP

The NAS-IP-Address field in the RADIUS accounting packet contains the IP address of the Network Management Ethernet (NME) port on the NSP, even if the NME is shutdown.

On an NSP that is preloaded with the Cisco IOS Release 12.0(5)DB or later software image, the combined NME interface is included in the default configuration. If your NRP does not use a DHCP server to obtain an IP address, you must configure a static IP address.

Note You must configure the NME IP address before configuring PVCs on the NRP. Otherwise, the NAS-IP-Address field in the RADIUS accounting packet will contain an incorrect IP address.

To configure a static combined NME IP address, enter the following commands beginning in global configuration mode:

Command	Purpose
`Switch(config)# interface BVI1`	Selects the combined NME interface.
`Switch(config-if)# ip address` *address subnet*	Configures a static IP and subnetwork address.

Instead of the combined NME interface, you can choose to use the Ethernet port as a separate NME interface. To configure the NME IP address, enter the following commands beginning in global configuration mode:

Command	Purpose
`Switch(config)# interface ethernet 0/0/0`	Selects the NME interface.
`Switch(config-if)# ip address` *address subnet* or `Switch(config-if)# ip address negotiated`	Configures a static IP and subnetwork address. Allows the interface to obtain an IP address, subnet mask, router address, and static routes from a DHCP server.

Verifying the NME Interface IP Address

To verify the NME IP address, enter the **show interface bvi1** or **show interface e0/0/0** EXEC command on the NSP. Check the Internet address statement (indicated with an arrow).

```
Switch# show interface bvi1
BVI1 is up, line protocol is up
  Hardware is BVI, address is 0010.7ba9.c783 (bia 0000.0000.0000)
➔   Internet address is 10.1.1.33/16
  MTU 1500 bytes, BW 10000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy:fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1540 packets input, 302775 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     545 packets output, 35694 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
Switch#
```

Task 2: Configuring RADIUS VC Logging on the NRP

To enable RADIUS VC logging on the Cisco 6400 NRP, enter the following command in global configuration mode:

Command	Purpose
`Router(config)# radius-server attribute nas-port format d`	Selects the ATM VC extended format for the NAS port field.

Verifying RADIUS VC Logging

To verify RADIUS VC Logging on the RADIUS server, examine a RADIUS accounting packet. If RADIUS VC logging is enabled on the Cisco 6400, the RADIUS accounting packet will appear similar to the following example:

```
Wed Jun 16 13:57:31 1999
NAS-IP-Address = 192.168.100.192
➔ NAS-Port = 268566560
NAS-Port-Type = Virtual
User-Name = "cisco"
Acct-Status-Type = Start
Service-Type = Framed
➔ Acct-Session-Id = "1/0/0/2.32_00000009"
Framed-Protocol = PPP
Framed-IP-Address = 172.16.7.254
Acct-Delay-Time = 0
```

The **NAS-Port** line shows that RADIUS VC logging is enabled. If this line does not appear in the display, then RADIUS VC logging is not enabled on the Cisco 6400.

The **Acct-Session-Id** line should also identify the incoming NSP interface and VPI/VCI information, in this format:

Acct-Session-Id = "*slot/subslot/port/VPI.VCI_acct-session-id*"

Note For soft PVCs, the Cisco 6400 returns the *egress* slot/subslot/port and VPI/VCI information in the **Acct-Session-Id** line.

Note The **NAS-IP-Address** line in the RADIUS accounting packet contains the IP address of the NME port on the NSP, even if the NME is shutdown. If the NME on the NSP does not have an IP address, this NAS-IP-Address field will contain “0.0.0.0.”

Task 3: Selecting the IP Address for RADIUS Attribute 4 (NAS-IP Address)

To select an IP address to be used as the source IP address for all outgoing RADIUS packets, enter the following commands in global configuration mode:

Command	Purpose
`Router(config)# ip radius source-interface int x`	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets
`Router(config)# radius-server attribute 4 nrp`	Allows the default-selected IP address to be changed. This command can only be enabled if "format d" is already configured.

The **ip radius source-interface** command specifies an interface to use for outgoing RADIUS packets. That interface must have an IP address configured in order for that IP address to be used as the source address for all outgoing RADIUS packets. The **radius-server attribute 4 nrp** command is used in combination with the commands in Table 6-4 to configure an IP address for that interface.

Table 6-4 RADIUS Global Configuration Commands and Selected IP Addresses

Global Configuration Commands			
ip radius source-interface <*int x*>	**radius-server attribute nas-port format d**	**radius-server attribute 4 nrp**	**Selected IP Address**
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 choice, 1st choice is loopback, etc.

Monitoring and Maintaining RADIUS VC Logging

Command	Purpose
`Router> show atm ingress [all | local-vc vpi/vci] [detailed]`	Displays ingress VC information of local VCs.

IPCP Subnet Mask Support

IPCP subnet mask support allows customer premises equipment (CPE) to connect to the Cisco 6400 node route processor (NRP) and obtain IP addresses and subnet mask ranges that the CPE can use to populate the Dynamic Host Configuration Protocol (DHCP) server database.

The Cisco 6400 brings up PPP sessions with the CPE and authenticates each CPE as a separate user. An extension of the normal IPCP negotiations enables the CPE to obtain an IP subnet mask associated with the returned IP address. The Cisco 6400 adds a static route for the IP address with the subnet mask specified.

If the subnet mask is specified by the Framed-IP-netmask attribute in the RADIUS user profile, the Cisco 6400 passes the mask and IP address to the CPE during IPCP negotiation. If the Framed-IP-netmask is not specified in the RADIUS user profile, the Cisco 6400 passes the subnet mask specified with the **ppp ipcp mask** command in the NRP configuration. If the subnet mask is not available from either the NRP configuration or the RADIUS user profile, the NRP rejects IPCP subnet mask negotiation from the CPE.

Note The subnet mask in the RADIUS user profile overrides the mask configured on the NRP.

The CPE uses the subnet mask to calculate an IP address pool from which IP addresses are assigned to PCs using the access link. Some CPE is hard-coded to request the subnet mask from the peer. If, however, the CPE uses Cisco IOS or CBOS, you must configure the CPE to support and initiate IPCP subnet mask negotiation.

Note Make sure you check and follow the documentation for your CPE software release. This section provides typical configuration guidelines for enabling CPE to support subnet mask negotiation.

IPCP subnet mask support configuration consists of the following tasks:

- Task 1 (Option 1): Configuring the Subnet Mask in the RADIUS User Profile
- Task 1 (Option 2): Configuring the Subnet Mask on the NRP
- Task 2 (Option 1): Configuring IPCP Subnet Mask Support on the Cisco IOS CPE
- Task 2 (Option 2): Configuring IPCP Subnet Mask Support on the CBOS CPE

Task 1 (Option 1): Configuring the Subnet Mask in the RADIUS User Profile

To configure the subnet mask in the RADIUS user profile, use the Framed-IP-netmask RADIUS IETF attribute.

Example—Configuring the Subnet Mask in the RADIUS User Profile

In the following example, the RADIUS user profile contains the netmask 255.255.255.248:

```
CPE1 Password = "cisco"
         Service-Type = Framed,
         Framed-Protocol = PPP,
         Framed-IP-Address=10.0.0.1
→        Framed-IP-netmask=255.255.255.248
         Framed-MTU = 1500
```

Verifying the Subnet Mask in the RADIUS User Profile

To verify the RADIUS user profile, refer to the user documentation for your RADIUS server.

You can also examine a RADIUS accounting packet and verify that the Framed-IP-netmask attribute is included in the packet:

```
Wed Jun 16 13:57:31 1999
NAS-IP-Address = 10.168.100.192


NAS-Port = 268566560
NAS-Port-Type = Virtual
User-Name = "cisco"
Acct-Status-Type = Start
Service-Type = Framed


Acct-Session-Id = "1/0/0/2.32_00000009"
Framed-Protocol = PPP
Framed-IP-Address = 10.16.7.254
➔ Framed-IP-netmask = 255.255.255.248
Acct-Delay-Time = 0
```

Task 1 (Option 2): Configuring the Subnet Mask on the NRP

You can configure a subnet mask on the NRP to send to the requesting peer, in case the RADIUS user profile does not include the Framed-IP-netmask attribute. On the NRP, the subnet mask is typically configured on a virtual template. Virtual templates are used to apply properties to PPP sessions.

To configure a subnet mask on the Cisco 6400 NRP, enter the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	`Router(config)# interface virtual template` *number*	Creates or specifies the virtual template interface. Enters interface configuration mode.
Step 2	`Router(config-if)# ppp ipcp mask` *subnet-mask*	Assigns the subnet mask to pass to a requesting peer (CPE).[1]

1. The subnet mask configured with the **ppp ipcp mask** command is passed to the requesting CPE only if the RADIUS user profile does not contain a subnet mask in the form of the Framed-IP-netmask attribute. If a subnet mask is not available from either the NRP configuration or the RADIUS user profile, the request is rejected.

Example—Configuring the Subnet Mask on the NRP

In the following 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 ATM0/0/0.30 multipoint
 pvc 1/43
  encapsulation aal5ciscoppp Virtual-Template 2
 !
!
interface Virtual-Template2
 ip unnumbered FastEthernet0/0/0
 no peer default ip address
 ppp authentication pap chap
 ppp ipcp mask 255.255.255.224
```

```
!
```

Verifying the Subnet Mask on the NRP

To verify that you successfully configured the subnet mask on the NRP, enter the **more system:running-config** EXEC command to display the current running configuration. Check that the **ppp ipcp mask** *subnet-mask* interface configuration command is applied to the appropriate virtual template.

Task 2 (Option 1): Configuring IPCP Subnet Mask Support on the Cisco IOS CPE

To configure the CPE to support and initiate IPCP subnet mask negotiation, complete the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	`CPE(config)# interface type number`	Selects the interface and interface type. Enters interface configuration mode.
Step 2	`CPE(config-if)# ppp ipcp mask request`	Specifies to request the subnet mask from the peer.

Example—Configuring IPCP Subnet Mask Support on the Cisco IOS CPE

In the following example, the CPE is configured to initiate IPCP subnet mask negotiation:

```
!
 interface Dialer 0
  ppp ipcp mask request
!
```

Task 2 (Option 2): Configuring IPCP Subnet Mask Support on the CBOS CPE

To configure the CPE to support and initiate IPCP subnet mask negotiation, enter the following commands in enable mode:

Command	Purpose
`cbos# set dhcp client enabled`	Enables the DHCP client.
`cbos# set dhcp server enabled`	Enables the DHCP server functionality.
`cbos# set dhcp server learn enabled`	Forces the server to use the IPCP negotiated address as the base IP address of its pool.
`cbos# set ppp wan0-0 subnet 0.0.0.0`	Enables the CPE to negotiate a subnet mask through IPCP during PPP negotiation.
`cbos# set ppp wan0-0 ipcp 0.0.0.0`	Enables the CPE to negotiate an IP address through IPCP during PPP negotiation.

Example—Configuring IPCP Subnet Mask Support on the CBOS CPE

In the following example, the CPE is configured to initiate IPCP subnet mask negotiation:

```
set dhcp client enabled
set dhcp server enabled
set dhcp server learn enabled
set nat disabled
set ppp wan0-0 login aladdin
set ppp wan0-0 password simsim
set ppp wan0-0 subnet 0.0.0.0
set ppp wan0-0 ipcp 0.0.0.0
write
set interface wan0 retrain
```

Verifying IPCP Subnet Mask Support on the CPE

Hard-Coded

To verify that your CPE is hard-coded to request the subnet mask from the peer, refer to the user documentation for your CPE.

Cisco IOS

To verify that you successfully configured IPCP subnet mask support, enter the **more system:running-config** EXEC command to display the current running configuration. Check that the **ppp ipcp mask request** interface configuration command is applied to the appropriate interface.

CBOS

To verify that you successfully configured IPCP subnet mask support, enter the **show dhcp server pool** *number* enable command. After negotiation, this command displays the IP address, subnet mask, pool start IP address and the pool size.

```
cbos# show dhcp server pool 0
  DHCP Server is currently disabled
  First pool will not learn IP address from IPCP
  Pool 0 currently enabled    Size 5
   IP Address: 10.1.1.9          Netmask:        255.255.255.248
   DNS Server: 0.0.0.0           Secondary DNS:  0.0.0.0
   WINS Server:0.0.0.0           Secondary WINS: 0.0.0.0
   Gateway   : 10.1.1.8          IRC Server:     0.0.0.0
   NNTP Server:0.0.0.0           Web Server:     0.0.0.0
   SMTP Server:0.0.0.0           POP3 Server:0.0.0.0
   Lease:      1080 seconds
cbos#
```

Troubleshooting IPCP Subnet Mask Support

To troubleshoot IPCP subnet mask support on the Cisco 6400 NRP, enter the following debug commands:

- **debug aaa authentication**—displays the methods and results of authentication being used
- **debug aaa authorization**—displays the methods and results of authorization being used
- **debug ppp negotiations**—displays the details of PPP/IPCP subnet negotiations

IP Overlapping Address Pools

IPCP IP pool processing implements all IP addresses as belonging to a single IP address space, and a given IP address should not be assigned multiple times. IP developments, such as VPDN and NAT implement the concept of multiple IP address spaces where it can be meaningful to reuse IP addresses, although such usage must ensure that these duplicate address are not placed in the same IP address space. This release introduces the concept of an IP address group to support multiple IP address spaces and still allow the verification of nonoverlapping IP address pools within a pool group. Pool names must be unique within the router. The pool name carries an implicit group identifier because that pool name can only be associated with one group. Pools without an explicit group name are considered members of the base system group and are processed in the same manner as the original IP pool implementation.

Existing configurations are not affected by the new pool feature. The "group" concept is an extension of the existing **ip local pool** command. Processing of pools that are not specified as a member of a group is unchanged from the existing implementation.

Benefits

This feature gives greater flexibility in assigning IP addresses dynamically. It allows you to configure overlapping IP address pool groups to create different address spaces and concurrently use the same IP addresses in different address spaces.

Restrictions

The software checks for duplicate addresses on a per-group basis. This means that you can configure pools in multiple groups that could have possible duplicate addresses. This feature should only be used in cases where Overlapping IP address pools make sense, such as MPLS VPN environments where multiple IP address spaces are supported.

Configuring a Local Pool Group for IP Overlapping Address Pools

To configure a local pool group, enter the following command in global configuration mode:

Command	Purpose
Router(config)# **ip local pool** *pool-name start-IP* [*end-IP*] [**group** *group-name*] [**cache-size** *size*]	Configures a group of local IP address pools. Optionally, this command names the group and specifies a cache size.

Example—Configuring IP Overlapping Address Pools

This example shows the configuration of two pool groups and includes 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
```

The 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).

The 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.

Verifying Local Pool Groups for IP Overlapping Address Pools

To verify that the new pool groups exist, enter the following command in privileged EXEC mode:

Command	Purpose
Router# **show ip local pool** [[**group** *group-name*] *pool-name*]	Displays local IP address pools.

Example—Displaying All IP Overlapping Address Pools

The following example displays all pools:

```
router# show 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
router#
```

Example—Displaying IP Address Pools in a Named Group

The following example displays the pools in the group named “mygroup”:

```
router# show 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
router#
```

ATM SNMP Trap and OAM Enhancements

The ATM SNMP Trap and OAM Enhancements feature introduces the following enhancements to the Simple Network Management Protocol (SNMP) notifications for ATM permanent virtual circuits (PVCs) and to operation, administration, and maintenance (OAM) functionality.

ATM PVC traps are now:

- Generated when the operational state of a PVC changes from the DOWN to UP state.
- Generated when OAM loopback fails. Additionally, when OAM loopback fails, the PVC will now remain in the UP state, rather than going DOWN.
- Extended to include:
  - VPI/VCI information
  - The number of state transitions a PVC goes through in an interval
  - The timestamp of the first and the last PVC state transition

The ATM SNMP Trap and OAM enhancements are described in the following sections:

ATM PVC UP Trap

Before the introduction of the ATM SNMP Trap and OAM enhancements, the only SNMP notifications for ATM PVCs were the ATM PVC DOWN traps, which were generated when a PVC failed or left the UP operational state. The ATM SNMP Trap and OAM enhancements introduce ATM PVC UP traps, which are generated when a PVC changes from the DOWN to UP state.

ATM PVC OAM Failure Trap

The ATM SNMP Trap and OAM enhancements also introduce the ATM PVC OAM failure trap. OAM loopback is a mechanism that detects whether a connection is UP or DOWN by sending OAM end-to-end loopback command/response cells. An OAM loopback failure indicates that the PVC has lost connectivity. The ATM PVC OAM failure trap is generated when OAM loopback for a PVC fails and is sent at the end of the notification interval.

When OAM loopback for a PVC fails, the PVC is included in the atmStatusChangePVclRangeTable or atmCurrentStatusChangePVclTable and in the ATM PVC OAM failure trap.

Before the introduction of this feature, if OAM loopback failed, the PVC would be placed in the DOWN state. When the ATM PVC OAM failure trap is enabled, the PVC remains UP when OAM loopback fails so that the flow of data is still possible.

Note 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.

Extended ATM PVC Traps

The ATM SNMP Trap and OAM enhancements introduce extended ATM PVC traps.

The extended traps include:

- VPI/VCI information for affected PVCs
- Number of UP-to-DOWN and DOWN-to-UP state transitions a PVC goes through in an interval
- Timestamp of the first and the last PVC state transition

Note 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.

Benefits

The ATM SNMP Trap and OAM enhancements:

- Enable you to use SNMP to detect the recovery of PVCs that have gone DOWN.
- Enable you to use SNMP to detect when OAM loopback for a PVC has failed.
- Keep the PVC in the UP state when OAM loopback has failed, allowing for the continued flow of data.
- Provide VPI/VCI information in the ATM PVC traps, so that you know which PVC has changed its operational state or has had an OAM loopback failure.
- Provide statistics on the number of state transitions a PVC goes through.

Restrictions

Note 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.

ATM PVC UP traps are not generated for newly created PVCs. They are only generated for PVCs that go from the DOWN to the UP state.

Prerequisites

Before you enable ATM PVC trap support, you must configure SNMP support and an IP routing protocol on your router. For more information about configuring SNMP support, refer to the chapter “Configuring SNMP Support” in the *Cisco IOS Configuration Fundamentals Configuration Guide*. For information about configuring IP routing protocols, refer to the section “IP Routing Protocols” in the *Cisco IOS IP Configuration Guide*.

To receive PVC failure notification and access to PVC status tables on your router, you must compile the Cisco extended ATM PVC trap MIB called CISCO-IETF-ATM2-PVCTRAP-MIB-EXTN.my in your NMS application. You can find this MIB on the Web at Cisco's MIB website:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Configuration Tasks

See the following sections for configuration tasks for the ATM SNMP Trap and OAM enhancements. Each task in the list is identified as either optional or required.

- Task 1: Configuring Extended ATM PVC Trap Support (required)
- Task 2: Enabling OAM Management (required)
- Verifying ATM PVC Traps (optional)

Task 1: Configuring Extended ATM PVC Trap Support

To configure extended ATM PVC trap support, use the following command in global configuration mode:

Command	Purpose
`Router(config)# snmp-server enable traps atm pvc extension {up | down | oam failure loopback}`	Enables the sending of extended ATM PVC traps. The keywords are as follows: • **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.

Task 2: Enabling OAM Management

When you configure PVC trap support, you must also enable OAM management on the PVC. To enable OAM management, use the following commands beginning in global configuration mode:

	Command	Purpose

Step 3	`Router(config)# interface atm slot/0[.subinterface-number {multipoint | point-to-point}]`
	or
	`Router(config)# interface atm slot/port-adapter/0[.subinterface-number {multipoint | point-to-point}]`
	or
	`Router(config)# interface atm number[.subinterface-number {multipoint | point-to-point}]`
		Specifies the ATM interface using the appropriate form of the **interface atm** command.[1]

Step 4	`Router(config-if)# pvc [name] vpi/vci`	Enables the PVC.
Step 5	`Router(config-if-atm-vc)# oam-pvc manage`	Enables end-to-end OAM management for an ATM PVC.

1. To determine the correct form of the **interface atm** command, refer to your ATM network module, port adapter, or router documentation.

Verifying ATM PVC Traps

To verify the configuration of ATM PVC traps, use the **show running-config** command. To view the status of ATM VCs, use the **show atm vc** command.

Example—Configuring Extended ATM PVC Trap Support

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
```

Monitoring and Maintaining ATM PVC Traps

To monitor ATM PVC trap performance, use the following commands in EXEC mode:

Command	Purpose
`Router# debug atm errors`	Displays ATM errors.
`Router# debug atm oam`	Displays information about ATM OAM events.
`Router# debug snmp packets`	Displays information about every SNMP packet sent or received by the router.

GLOSSARY

A

AAA authentication, authorization, and accounting (pronounced "triple a").

address mask A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Sometimes called subnet mask.

AAL5 ATM Adaptation Layer. This layer maps higher layer user data into ATM cells, making the data suitable for transport through the ATM network.

ADSL Asymmetric digital subscriber line. A digital subscriber line (DSL) technology in which the transmission of data from server to client is much faster than the transmission from the client to the server.

ATM Asynchronous Transfer Mode. International standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media such as E3, SONET, and T3.

authentication A security feature that allows access to information to be granted on an individual basis.

auto-negotiation Procedure for adjusting line speeds and other communication parameters automatically between two computers during data transfer.

B

bandwidth The range of frequencies a transmission line or channel can carry: the greater the bandwidth, the greater the information-carrying capacity of a channel. For a digital channel this is defined in bits. For an analog channel it is dependent on the type and method of modulation used to encode the data.

bandwidth-on-demand The ability of a user to dynamically set upstream and downstream line speeds to a particular speed.

bps Bits per second. A standard measurement of digital transmission speeds.

bridge A device that connects two or more physical networks and forwards packets between them. Bridges can usually be made to filter packets, that is, to forward only certain traffic. Related devices are: repeaters which simply forward electrical signals from one cable to the other, and full-fledged routers which make routing decisions based on several criteria. See repeater and router.

B

broadband Characteristic of any network that multiplexes independent network carriers onto a single cable. This is usually done using frequency division multiplexing (FDM). Broadband technology allows several networks to coexist on one single cable; traffic from one network does not interfere with traffic from another because the "conversations" happen on different frequencies in the "ether" rather like the commercial radio system.

Broadband Remote Access Server Device that terminates remote users at the corporate network or Internet users at the Internet service provider (ISP) network, that provides firewall, authentication, and routing services for remote users.

broadcast A packet delivery system where a copy of a given packet is given to all hosts attached to the network. Example: Ethernet.

C

CBOS Cisco Broadband Operating System. The common operating system for DSL CPE, including the Cisco 675, the Cisco 675e, the Cisco 676, and the Cisco 677.

CO Central office. Refers to equipment located at a Telco or service provider's office.

CEF Cisco Express Forwarding. Advanced Layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as the Internet, on networks characterized by intensive Web-based applications, or interactive sessions.

CHAP Challenge Handshake Authentication Protocol. Security feature supported on lines using PPP encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access; it merely identifies the remote end. The router or access server then determines whether that user is allowed access. Compare to PAP.

CPE Customer premises equipment. Refers to equipment located in a user's premises.

D

DHCP Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

DNS Domain Name Server. The part of the distributed database system for resolving a fully qualified domain name into the four-part IP (Internet Protocol) number used to route communications across the Internet.

downstream rate The line rate for return messages or data transfers from the network machine to the user's customer premises machine.

DRAM Dynamic Random Access Memory. A type of semiconductor memory in which the information is stored in capacitors on a metal oxide semiconductor integrated circuit.

DSLAM Digital Subscriber Line Access Multiplexer. Concentrates and multiplexes signals at the telephone service provider location to the broader wide area network.

E

encapsulation The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the physical layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data.

Ethernet One of the most common local area network (LAN) wiring schemes, Ethernet has a transmission rate of 10, 100, or 1000 Mbps.

F

Fast switching Cisco feature whereby a route cache is used to expedite packet switching through a router.

FCC Federal Communications Commission. A U.S. government agency that regulates interstate and foreign communications. The FCC sets rates for communication services,

FTP File Transfer Protocol. The Internet protocol (and program) used to transfer files between hosts.

H

hop count A measure of distance between two points on the Internet. It is equivalent to the number of gateways that separate the source and destination.

HTML Hypertext Markup Language. The page-coding language for the World Wide Web.

HTML browser A browser used to traverse the Internet, such as Netscape or Microsoft Internet Explorer.

http Hypertext Transfer Protocol. The protocol used to carry world-wide web (www) traffic between a www browser computer and the www server being accessed.

I

ICMP Internet Control Message Protocol. The protocol used to handle errors and control messages at the IP layer. ICMP is actually part of the IP protocol.

Internet address An IP address assigned in blocks of numbers to user organizations accessing the Internet. These addresses are established by the United States Department of Defense's Network Information Center. Duplicate addresses can cause major problems on the network, but the NIC trusts organizations to use individual addresses responsibly. Each address is a 32-bit address in the form of x.x.x.x where *x* is an eight- bit number from 0 to 255. There are three classes: A, B and C, depending on how many computers on the site are likely to be connected.

IETF Internet Engineering Task Force. Task force consisting of over 80 working groups responsible for developing Internet standards. The IETF operates under the auspices of ISOC. See also ISOC.

I

IGMP Internet Group Management Protocol. Used by IP hosts to report their multicast group memberships to an adjacent multicast router.

inform An SNMP trap message which includes a delivery confirmation request. See "trap."

Internet A collection of networks interconnected by a set of routers which allow them to function as a single, large virtual network. When written in upper case, Internet refers specifically to the DARPA (Defense Advanced Research Projects Agency) Internet and the TCP/IP protocols it uses.

Internet Protocol (IP) The network layer protocol for the Internet protocol suite.

IRB Integrated routing and bridging. A protocol that allows a router to act as both bridge and router on the same interface. For broadband aggregation, Cisco recommends using the routed bridge encapsulation (RBE) protocol. See RBE.

IP See Internet Protocol.

IP address The 32-bit address assigned to hosts that want to participate in a TCP/IP Internet.

IPCP IP Control Protocol. Protocol that establishes and configures IP over PPP.

IP datagram The fundamental unit of information passed across the Internet. It contains source and destination addresses along with data and a number of fields that define such things as the length of the datagram, the header checksum, and flags to say whether the datagram can be or has been fragmented.

ISO International Standards Organization. A voluntary, non-treaty organization founded in 1946, responsible for creating international standards in many areas, including computers and communications.

ISP Internet service provider. A company that allows home and corporate users to connect to the Internet.

ITU-T International Telecommunications Union, Standardization Sector. ITU-T is the telecommunication standardization sector of ITU and is responsible for making technical recommendations about telephone and data (including fax) communications systems for service providers and suppliers.

L

L2F Layer 2 Forwarding. Protocol that supports the creation of secure virtual private dial-up networks over the Internet.

L2TP Layer 2 Tunnel Protocol. An Internet Engineering Task Force (IETF) standards track protocol defined in RFC 2661 that provides tunneling of PPP. Based upon the best features of L2F and PPTP, L2TP provides an industry-wide interoperable method of implementing VPDN.

LAC L2TP access concentrator. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP network server (LNS). The LAC sits between an LNS and a remote system and forwards packets to and from each. Packets sent from the LAC to the LNS requires tunneling with the L2TP protocol as defined in this document. The connection from the LAC to the remote system is either local or a PPP link.

L

LAN Local area network. A limited distance (typically under a few kilometers or a couple of miles) high-speed network (typically 4 to 100 Mbps) that supports many computers.

LCP link control protocol. Protocol that establishes, configures, and tests data-link connections for use by PPP.

LED Light emitting diode. The lights indicating status or activity on electronic equipment.

line rate The speed by which data is transferred over a particular line type, expressed in bits per second (bps).

LNS L2TP network server. A node that acts as one side of an L2TP tunnel endpoint and is a peer to the L2TP access concentrator (LAC). The LNS is the logical termination point of a PPP session that is being tunneled from the remote system by the LAC. Analogous to the Layer 2 Forwarding (L2F) home gateway (HGW).

logical port A logical entry to a server machine. These ports are mostly invisible to the user, though you might occasionally see a URL with a port number included in it. These ports do not refer to physical locations; they are set up by server administrators for network trafficking.

loopback A diagnostic test that returns the transmitted signal back to the sending device after it has passed through a network or across a particular link. The returned signal can then be compared to the transmitted one. The discrepancy between the two helps to trace the fault. When trying to locate a faulty piece of equipment, loopbacks will be repeated, eliminating satisfactory machines until the problem is found.

LSC Label switch controller.

LSR Label switch router.

M

MAC Media Access Control Layer. A sublayer of the Data Link Layer (Layer 2) of the ISO OSI Model responsible for media control.

MIB Management Information Base. Database of network management information that is used and maintained by a network management protocol, such as SNMP or CMIP (Common Management Information Protocol). The value of a MIB object can be changed or retrieved using SNMP commands, usually through a Network Management System (NMS). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

modem pooling The ability of a service provider to dynamically switch users' messages between modems, rather than requiring a modem to be dedicated to a particular user on a network.

MPLS Multiprotocol Label Switching. Emerging industry standard upon which tag switching is based.

M

multicast Single packets copied by the network and sent to a specific subset of network addresses. These addresses are specified in the Destination Address Field.

multiplexer A device that can send several signals over a single line. The signals are then separated by a similar device at the other end of the link. This can be done in a variety of ways: time division multiplexing, frequency division multiplexing, and statistical multiplexing. Multiplexers are also becoming increasingly efficient in terms of data compression, error correction, transmission speed, and multi-drop capabilities.

N

NAS network access server. A device providing local network access to users across a remote access network such as the PSTN.

NAT Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.

network layer The OSI layer that is responsible for routing, switching, and subnetwork access across the entire OSI environment.

NME network management Ethernet. The local area network used to control and manage equipment in a central office and branch locations. The NME connection on the Cisco 6400 is an RJ-45 connector for a 10BaseT port on the NSP module.

NMS network management system. An application or suite of applications designed to monitor networks using SNMP. CiscoView is one example of an NMS.

node A general term used to refer to a computer or related device; often used to refer to a networked computer or device.

NRP node route processor. One of the component modules used in the Cisco 6400. This module is the Layer 3 element for the Cisco 6400 responsible for implementing the routing function.

NRP-1 Node route processor that incorporates a 100-Mbps Fast Ethernet interface for connecting into an IP network and has processing capability for OC-3 rate of user traffic. Compare with NRP-2.

NRP-2 Node route processor that provides a Gigabit Ethernet interface and sufficient processing capability for handling OC-12 rate of user traffic. Compare with NRP-1.

NSP node switch processor. One of the component modules used in the Cisco 6400. This module is responsible for all ATM switching and control functions within the Cisco 6400.

NVRAM Non-Volatile Random Access Memory. The router uses this memory to store configuration information. The contents of this memory are not lost after a reboot or power cycle of the unit.

O

octet A networking term that identifies 8 bits. In TCP/IP, it is used instead of *byte*, because some systems have bytes that are not 8 bits.

OSI Open Systems Interconnection. An international standardization program to facilitate communications among computers from different manufacturers. See ISO.

OAP Overlapping Address Pool. An IP address group that supports multiple IP address spaces and still allows for the verification of nonoverlapping IP address pools within a pool group.

P

packet The unit of data sent across a packet switching network.

PAP Password Authentication Protocol. Authentication protocol that allows PPP peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike CHAP, PAP passes the password and host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines if that user is allowed access. PAP is supported only on PPP lines. Compare with CHAP.

PCI Peripheral Component Interconnect. An industry local bus standard. Supports up to 16 physical slots but is electrically limited to typically three or four plug-in PCI cards in a PC. Has a typical sustained burst transfer rate of 80 Mbps, which is enough to handle 24-bit color at 30 frames per second (full-color, full-motion video).

Permanent Virtual Connection (PVC) A fixed virtual circuit between two users: the public data network equivalent of a leased line. No call setup or clearing procedures are needed.

physical layer Handles transmission of raw bits over a communication channel. The physical layer deals with mechanical, electrical, and procedural interfaces.

physical port A physical connection to a computer through which data flows. An “Ethernet port,” for example, is where Ethernet network cabling plugs in to a computer.

POP point of presence. Physical location within a LATA where a long distance carrier or cellular provider interfaces with the network of the local exchange carrier (LEC), also called the local telephone company.

port The abstraction used by Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host. See selector.

POTS Plain Old Telephone Service. This is the term used to describe basic telephone service.

PPP Point-to-Point-Protocol. The successor to SLIP, PPP provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits. See SLIP.

PPPoA PPP over ATM.

PPPoE PPP over Ethernet.

P

protocol A formal description of messages to be exchanged and rules to be followed for two or more systems to exchange information.

PTA PPP termination aggregation. A method of aggregating IP traffic by terminating PPP sessions and aggregating the IP traffic into a single routing domain.

PTA-MD PTA Multi-Domain. A method of aggregating IP traffic by terminating PPP sessions and aggregating the IP traffic into a VPN or multiple IP routing domains.

PVC permanent virtual circuit or connection. Virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time. In ATM terminology, called a permanent virtual connection. Compare with SVC. See also virtual circuit (VC).

PVP permanent virtual path. Virtual path that consists of PVCs. See also PVC and virtual path.

R

RADIUS Remote Authentication Dial-In User Service (RADIUS). A client/server security protocol created by Livingston Enterprises. Security information is stored in a central location, known as the RADIUS server.

RADIUS Accounting Client Permits system administrators to track dial-in use.

RADIUS Security Client Controls access to specific services on the network.

RADSL Rate Adaptive Digital Subscriber Line (RADSL). A technique for keeping the quality of transmissions within specified parameters.

RBE routed bridge encapsulation. The process by which a stub-bridged segment is terminated on a point-to-point routed interface. Specifically, the router is routing on an IEEE 802.3 or Ethernet header carried over a point-to-point protocol such as PPP, RFC 1483 ATM, or RFC 1490 Frame Relay.

remote address The IP address of a remote server.

remote server A network computer that allows a user to log on to the network from a distant location.

RFC Request for Comments. The document series, begun in 1969, which describes the Internet suite of protocols and related experiments. Not all RFCs describe Internet standards, but all Internet standards are written up as RFCs.

route The path that network traffic takes from its source to its destination. The route a datagram follows can include many gateways and many physical networks. In the Internet, each datagram is routed separately.

router A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. To do this, it uses a routing protocol to gain information about the network and algorithms to choose the best route based on several criteria known as “routing metrics.” See bridge and repeater.

R

routing table Information stored within a router that contains network path and status information. It is used to select the most appropriate route to forward information along.

RS-232 An EIA standard that is the most common way of linking data devices together.

S

SDSL Symmetrical digital subscriber line. A digital subscriber line (DSL) technology in which the transmission of data from server to client is the same speed as the transmission from the client to the server.

secret Encryption key used by RADIUS to send authentication information over a network.

serial line A serial line is used to refer to data transmission over a telephone line via a modem or when data goes from a computer to a printer or other device.

shared secret RADIUS uses the shared secret to encrypt the passwords in the authentication packets, so outside parties do not have access to the passwords on your network.

SNAP Subnetwork Access Protocol. Internet protocol that operates between a network entity in the subnetwork and a network entity in the end system. SNAP specifies a standard method of encapsulating IP datagrams and ARP messages on IEEE networks.

SNMP Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security, typically through the use of an NMS.

socket (1) The Berkeley UNIX mechanism for creating a virtual connection between processes. (2) IBM term for software interfaces that allow two UNIX application programs to talk via TCP/IP protocols.

spoofing A method of fooling network end stations into believing that keepalive signals have come from and returned to the host. Polls are received and returned locally at either end of the network and are transmitted only over the open network if there is a condition change.

SSD The Service Selection Dashboard (SSD) server is a customizable Web-based application that works with the Cisco SSG to allow end customers to log on to and disconnect from proxy and passthrough services through a standard Web browser. After the customer logs in to the service provider's network, an HTML Dashboard is populated with the services authorized for that user.

SSG Service Selection Gateway. The Cisco SSG offers service providers a means for menu-based service selection. End users can select services from the Dashboard menu, and the Cisco SSG will set up and tear down proxy and passthrough network connections based on a user's selection. The Cisco SSG will account for the services selected so that service providers can bill for individual services.

subnet For routing purposes, IP networks can be divided into logical subnets by using a subnet mask. Values below those of the mask are valid addresses on the subnet.

subnet mask 32-bit address mask used in IP to indicate the bits of an IP address that are being used for the subnet address.

S

SVC switched virtual circuit. Virtual circuit that is dynamically established on demand and is torn down when transmission is complete. SVCs are used in situations where data transmission is sporadic. Called a switched virtual connection in ATM terminology. Compare with PVC.

synchronous connection During synchronous communications, data is not sent in individual bytes, but as frames of large data blocks.

SYSLOG SYSLOG allows you to log significant system information to a remote server.

T

TACACS+ Terminal Access Controller Access Control System Plus. Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting.

TCP Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack. See also TCP/IP.

TCP/IP Transmission Control Protocol/Internet Protocol. Common name for the suite of protocols developed by the U.S. DoD in the 1970s to support the construction of worldwide internetworks. TCP and IP are the two best-known protocols in the suite.

TFTP Trivial File Transfer Protocol. A simple file transfer protocol (a simplified version of FTP) that is often used to boot diskless workstations and other network devices such as routers over a network (typically a LAN). Has no password security.

Telnet The virtual terminal protocol in the Internet suite of protocols. Allows users of one host to log into a remote host and act as normal terminal users of that host.

transparent bridging So named because the intelligence necessary to make relaying decisions exists in the bridge itself and is thus transparent to the communicating workstations. It involves frame forwarding, learning workstation addresses and ensuring no topology loops exist (in conjunction with the Spanning-Tree algorithm).

trap Message sent by an SNMP agent to a network management station, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.

Trivial File Transfer Protocol See TFTP.

U

UDP User Datagram Protocol. A connectionless transport protocol that runs on top of TCP/IP's IP. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagrams without acknowledgments or guaranteed delivery. Best suited for small, independent requests, such as requesting a MIB value from an SNMP agent, in which first setting up a connection would take more time than sending the data.

UNI signaling User Network Interface signaling for ATM communications.

upstream rate The line rate for message or data transfer from the source machine to a destination machine on the network. Also see downstream rate.

V

VC See Virtual Connection.

VCI virtual channel identifier. 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through a s series of ATM switches on its way to its destination. ATM switches use the VPI/VCI fields to identify the next network VCL that a cell needs to transmit on its way to its final destination. The function of the VCI is similar to that of the DLCI in Frame Relay.

Virtual Connection (VC) A link that seems and behaves like a dedicated point-to-point line or a system that delivers packets in sequence, as happens on an actual point-to-point network. In reality, the data is delivered across a network via the most appropriate route. The sending and receiving devices do not have to be aware of the options and the route is chosen only when a message is sent. There is no pre-arrangement, so each virtual connection exists only for the duration of that one transmission.

VIP Virtual Ethernet Interface.

VLAN virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VPDN Virtual Private Dial-Up Networking. A system that permits dial-in networks to exist remotely to home networks, while giving the appearance of being directly connected. VPDNs use L2TP and L2F to terminate the Layer 2 and higher parts of the network connection at the home gateway, instead of the NAS.

VPI virtual path identifier. 8-bit field in the header of an ATM cell. The VPI, together with the VCI, is used to identify the next destination of a cell as it passes through a s series of ATM switches on its way to its destination. ATM switches use the VPI/VCI fields to identify the next VCL that a cell needs to transmit on its way to its final destination. The function of the VPI is similar to that of the DLCI in Frame Relay.

VPN Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

W

WAN Wide area network. A data communications network that spans any distance and is usually provided by a public carrier (such as a telephone company or service provider).

X

xDSL Various types of digital subscriber lines. Examples include ADSL, HDSL, and VDSL.

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W