



Cisco 6400 Feature Guide -- Release 12.2(2)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-0875-04

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0201R)

Cisco 6400 Feature Guide -- Release 12.2(2)B
Copyright © 2001-2002, Cisco Systems, Inc.
All rights reserved.



Preface **xiii**

How to Use This Guide	xiii
Document Objectives	xiii
Related Documentation	xiii
Audience	xiii
Document Organization	xiii
Document Conventions	xiv
Obtaining Documentation	xv
World Wide Web	xv
Documentation CD-ROM	xv
Ordering Documentation	xv
Documentation Feedback	xvi
Obtaining Technical Assistance	xvi
Cisco.com	xvi
Technical Assistance Center	xvii

Supported Features **1-1**

Conventions Used in This Chapter	1-2
Node Route Processor Features	1-2
Access Protocols	1-3
Aggregation and Virtual Private Networks (VPNs)	1-5
Configuration and Monitoring	1-7
Hardware Support	1-7
IP and Routing	1-8
IP QoS	1-10
Network Management	1-10
RADIUS/AAA	1-11
Scalability and Performance	1-12
Service Selection Gateway (NRP-SSG)	1-13
Other Features and Feature Enhancements	1-16

- Node Switch Processor Features **1-17**
 - ATM Connections **1-17**
 - ATM Internetworking **1-18**
 - ATM Per-Flow Queuing **1-18**
 - ATM Traffic Classes **1-19**
 - Configuration and Monitoring **1-20**
 - Hardware Support **1-21**
 - IP and Routing **1-22**
 - Network Management **1-22**
 - RADIUS/AAA **1-23**
 - Scalability and Performance **1-23**
 - Signaling and Routing **1-23**

Layer 2 Tunnel Protocol 2-1

- Overview **2-1**
- Restrictions **2-1**
- L2TP Scalability Prerequisites **2-1**
- Configuring L2TP **2-2**
 - Configuring VPDN on the LAC **2-2**
 - Configuring VPDN on the LNS **2-3**
 - Tunnel Service Authorization **2-4**
 - Sessions per Tunnel Limiting **2-9**
 - Tunnel Sharing **2-12**
 - Tunnel Switching **2-14**
- Monitoring and Troubleshooting VPDN and L2TP **2-20**

Multiprotocol Label Switching 3-1

- Restrictions **3-1**
- Prerequisites **3-1**
- MPLS Edge Label Switch Router **3-2**
 - MPLS Edge LSRs Connected Through a PVP **3-3**
 - MPLS Edge LSRs Connected Through a VPI Range **3-5**
- MPLS Virtual Private Networks **3-7**
 - Basic MPLS VPN Configuration Example **3-7**
 - Split Horizon and RIP Example **3-16**

Service Selection Gateway	4-1
Overview	4-1
Benefits	4-4
Restrictions	4-10
Prerequisites	4-11
Configuring Features	4-11
Enabling SSG	4-12
Configuring Local Service Profiles	4-12
Configuring Security	4-13
Configuring a Default Network	4-13
Configuring Interfaces	4-14
Configuring Services	4-15
Configuring Fastswitching	4-15
Configuring Multicast	4-16
Configuring RADIUS Interim Accounting	4-16
Configuring Cisco Express Forwarding	4-17
Configuring IOS Network Address Translation	4-17
Configuring VPI/VCI Indexing to Service Profile	4-18
Configuring SSG with L2TP Service Type	4-19
Configuring Local Forwarding	4-23
Configuring an Open Garden	4-24
Configuring TCP Redirect - Logon	4-26
Configuring Host Key	4-28
Configuring AAA Server Group Support for Proxy Services	4-32
Configuring the Proxy RADIUS Enhancements	4-33
RADIUS Accounting Records	4-34
Account Logon	4-35
Account Logoff	4-35
Connection Start	4-36
Connection Stop	4-36
Attributes Used in Accounting Records	4-37
Configuring RADIUS Profiles	4-39
SSG Vendor-Specific Attributes	4-40
User Profiles	4-42
Service Profiles	4-46
Service Group Profiles	4-56
Pseudo-Service Profiles	4-59

- Configuration Example **4-62**
 - Security **4-63**
 - Default Network **4-63**
 - Interfaces **4-63**
 - Services **4-64**
 - Service Search Order **4-64**
 - Next-Hop Table **4-64**
 - Max Services **4-65**
 - Local Service Profile **4-65**
 - Transparent Passthrough Filter **4-65**
 - Redundancy **4-65**
 - Fastswitching **4-65**
 - Multicast **4-65**
 - RADIUS Interim Accounting **4-66**
 - CEF **4-66**
 - IOS NAT **4-66**
 - Service Name to VC Mapping **4-67**
- Monitoring and Troubleshooting SSG **4-67**
 - RADIUS **4-68**

Point-to-Point Protocol 5-1

- Restrictions **5-1**
- Prerequisites **5-1**
- Configuration Tasks **5-1**
 - Configuring PPPoA **5-2**
 - Configuring PPPoE **5-5**
 - Configuring PPP Autosense **5-9**
 - Configuring AAA Authentication **5-13**
 - Configuring PPPoE Session Limit **5-15**
 - Configuring PPPoE Session Count MIB **5-19**

Session and Tunnel Scalability 6-1

- Recommendations **6-1**
- Restrictions **6-2**
- Input and Output Hold-Queues **6-2**
 - Configuring the Input or Output Hold-Queue Limit **6-3**
 - Verifying the Input and Hold-Queue Limits **6-3**
- LCP Session Initiations **6-3**
 - Limiting the Number of Simultaneous LCP Session Initiations **6-4**
 - Verifying the Simultaneous LCP Session Initiation Limit **6-4**

PPP Timeouts	6-4
Configuring the PPP Timeouts	6-5
Verifying the PPP Timeouts	6-5
Keepalives	6-5
Configuring the Interface Keepalive Interval	6-6
Verifying the Interface Keepalive Interval	6-6
Configuring the L2TP Tunnel Keepalive Interval	6-7
Verifying the L2TP Tunnel Keepalive Interval	6-7
Virtual Access Interface Precloning	6-7
Precloning Virtual Access Interfaces	6-7
Verifying the Precloned Virtual Access Interfaces	6-8
L2TP Control Channel Parameters	6-8
Configuring the Control Channel Retransmission Parameters	6-8
Verifying the Control Channel Retransmission Parameters	6-9
Configuring the Local Control Channel Receive Window Size	6-9
Verifying the Local Control Channel Receive Window Size	6-9
L2TP Tunnel Timeout	6-10
Configuring the L2TP Tunnel Timeout	6-10
Verifying the L2TP Tunnel Timeout	6-10
An Example Configuration of Session and Tunnel Scalability Parameters	6-10
Monitoring and Troubleshooting PPP Scalability	6-11
Monitoring and Troubleshooting L2TP Scalability	6-12
Miscellaneous Features	6-1
Routing and Bridging	6-1
ATM Routed Bridge Encapsulation	6-3
Benefits	6-3
Restrictions	6-4
Configuration Tasks	6-4
Routed Bridge Encapsulation for Cisco Express Forwarding	6-5
RADIUS VC Logging	6-6
Configuring RADIUS VC Logging	6-6
Monitoring and Maintaining RADIUS VC Logging	6-9
IPCP Subnet Mask Support	6-9
Configuring the Subnet Mask	6-9
Configuring IPCP Subnet Mask Support on the CPE	6-11

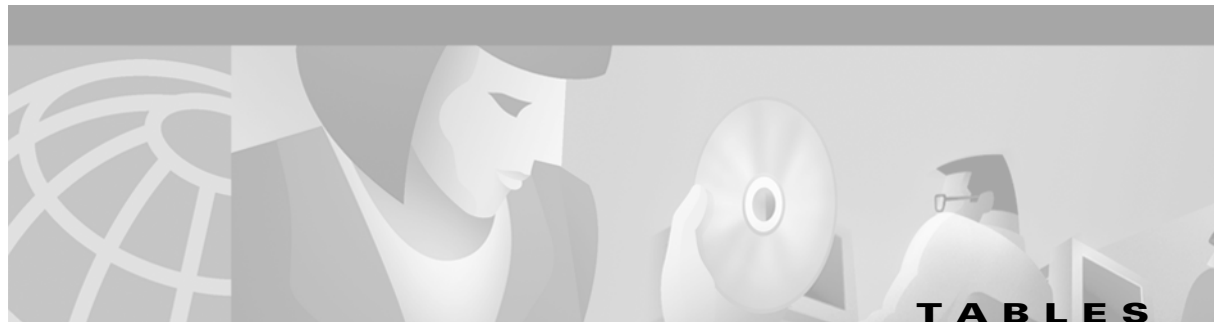
- IP Overlapping Address Pools **6-13**
 - Benefits **6-14**
 - Restrictions **6-14**
 - Configuring a Local Pool Group for IP Overlapping Address Pools **6-14**
- ATM SNMP Trap and OAM Enhancements **6-15**
 - Restrictions **6-17**
 - Prerequisites **6-17**
 - Configuration Tasks **6-17**

GLOSSARY

INDEX

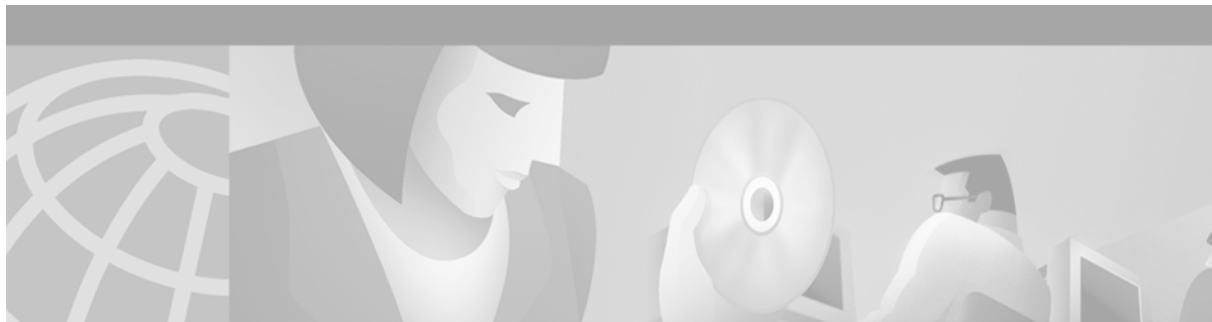


<i>Figure 2-1</i>	Example Network Topology Using the L2TP Tunnel Switching Feature	2-15
<i>Figure 2-2</i>	Example L2TP Tunnel Switch Topology	2-18
<i>Figure 3-1</i>	PVP Connection Between Two Edge LSRs Within a Cisco 6400	3-3
<i>Figure 3-2</i>	PVP Connection Between Two Edge LSRs in Separate Cisco 6400s	3-4
<i>Figure 3-3</i>	VPI Range Between Two Edge LSRs Within a Cisco 6400	3-5
<i>Figure 3-4</i>	VPI Range Between Two NRPs in Different Cisco 6400s	3-6
<i>Figure 3-5</i>	Basic Cisco 6400 MPLS VPN Topology	3-8
<i>Figure 3-6</i>	Detailed Schematic of the MPLS VPN Configuration Shown in Figure 3-5	3-9
<i>Figure 4-1</i>	SSG Connection Between ADSL Equipment and Network Services	4-3
<i>Figure 4-2</i>	Example SSG Network Topology	4-63
<i>Figure 7-1</i>	ATM Routed Bridge Encapsulation	6-3



<i>Table 1</i>	Font Conventions	xiv
<i>Table 2</i>	Command Syntax Conventions	xiv
<i>Table 3</i>	Note, Timesaver, Tip, Caution, and Warning Conventions	xv
<i>Table 1-1</i>	Examples of Conventions Used in the “Supported Features” Chapter	1-2
<i>Table 1-2</i>	NRP Features—Access Protocols	1-3
<i>Table 1-3</i>	NRP Features—Aggregation and VPNs	1-5
<i>Table 1-4</i>	NRP Features—Configuration and Monitoring	1-7
<i>Table 1-5</i>	NRP Features—Hardware Support	1-7
<i>Table 1-6</i>	NRP Features—IP and Routing	1-8
<i>Table 1-7</i>	NRP Features—IP QoS	1-10
<i>Table 1-8</i>	NRP Features—Network Management	1-10
<i>Table 1-9</i>	NRP Features—RADIUS/AAA	1-11
<i>Table 1-10</i>	NRP Features—Scalability and Performance	1-12
<i>Table 1-11</i>	NRP Features—SSG	1-13
<i>Table 1-12</i>	NRP Features—Other Features and Feature Enhancements	1-16
<i>Table 1-13</i>	NSP Features—ATM Connections	1-17
<i>Table 1-14</i>	NSP Features—ATM Internetworking	1-18
<i>Table 1-15</i>	NSP Features—ATM Per-Flow Queuing	1-18
<i>Table 1-16</i>	NSP Features—ATM Traffic Classes	1-19
<i>Table 1-17</i>	NSP Features—Configuration and Monitoring	1-20
<i>Table 1-18</i>	NSP Features—Hardware Support	1-21
<i>Table 1-19</i>	NSP Features—IP and Routing	1-22
<i>Table 1-20</i>	NSP Features—Network Management	1-22
<i>Table 1-21</i>	NSP Features—RADIUS/AAA	1-23
<i>Table 1-22</i>	NSP Features—Scalability and Performance	1-23
<i>Table 1-23</i>	NSP Features—Signaling and Routing	1-23
<i>Table 2-1</i>	show vpdn tunnel all Field Descriptions	2-20
<i>Table 2-2</i>	VPDN Monitoring and Maintaining Commands	2-21
<i>Table 2-3</i>	VPDN Troubleshooting Commands	2-21
<i>Table 4-1</i>	Cisco AVPair Attributes	4-20
<i>Table 4-2</i>	Account-Info Attribute	4-20

<i>Table 4-3</i>	Service-Info Attributes	4-20
<i>Table 4-4</i>	Port-Bundle Lengths and Resulting Port per Bundle and Bundle per Group Values	4-30
<i>Table 4-5</i>	Service-Info VSA Used to Configure AAA Server Group Support for Proxy Services	4-32
<i>Table 4-6</i>	Service-Info VSAs Introduced by the Proxy RADIUS Enhancements	4-33
<i>Table 4-7</i>	Vendor-Specific RADIUS Attributes for the SSG	4-40
<i>Table 4-8</i>	Cisco-AVPair Attributes	4-40
<i>Table 4-9</i>	Account-Info Attributes	4-41
<i>Table 4-10</i>	Service-Info Attributes	4-41
<i>Table 4-11</i>	Control-Info Attribute	4-42
<i>Table 4-12</i>	User Profile Attributes	4-43
<i>Table 4-13</i>	Service Profile Attributes	4-47
<i>Table 4-14</i>	Service Group Profile Attributes	4-57
<i>Table 4-15</i>	Transparent Passthrough Filter Pseudo-Service Profile Attributes	4-59
<i>Table 4-16</i>	Next Hop Gateway Pseudo-Service Profile Attributes	4-61
<i>Table 4-17</i>	SSG Monitoring and Troubleshooting Commands	4-67
<i>Table 5-1</i>	PPPoE Monitoring and Maintaining Commands	5-9
<i>Table 5-2</i>	PPPoA Monitoring and Maintaining Commands	5-13
<i>Table 5-3</i>	PPPoE Session Count MIB Objects and Tables.	5-20
<i>Table 6-1</i>	Default Input and Output Hold-Queue Limits	6-2
<i>Table 6-2</i>	Scalability-Related show vpdn tunnel all Field Descriptions	6-13
<i>Table 7-1</i>	RADIUS Global Configuration Commands and Selected IP Addresses	6-9



Preface

How to Use This Guide

To obtain information about features of the Cisco 6400 carrier-class broadband aggregator supported in Cisco IOS Release 12.2(2)B, see Chapter 1, “Supported Features.” Find the feature that you want and follow the link to other sections of this guide or other documents for detailed information about the feature.

Document Objectives

The objectives of this guide are to describe the software features and basic configuration procedures for the Cisco 6400.

Related Documentation

Use this guide with the following documentation:

- *Cisco 6400 Software Setup Guide*
- *Cisco 6400 Command Reference*

Audience

This guide is developed for system and network managers.

Document Organization

Chapter	Title	Topics Described
Chapter 1	Supported Features	Describes features supported in Cisco IOS Release 12.2(2)B and where to find feature information.
Chapter 2	Layer 2 Tunnel Protocol	Describes L2TP features.

Chapter	Title	Topics Described
Chapter 3	Multiprotocol Label Switching	Describes MPLS features.
Chapter 4	Service Selection Gateway	Describes SSG features.
Chapter 5	Point-to-Point Protocol	Describes PPP features.
Chapter 6	Session and Tunnel Scalability	Describes session and tunnel scalability parameters.
Chapter 7	Miscellaneous Features	Describes miscellaneous features
Glossary	—	Provides technology definitions.

Document Conventions





Table 1 Font Conventions

Convention	Definition	Sample
Times bold	Text body font used for arguments, commands, keywords, and punctuation that is part of a command that the user enters in text and command environments.	This is similar to the UNIX route command.
<i>Times italic</i>	Text body font used for publication names and for emphasis.	Refer to the <i>Cisco Broadband Operating System UserGuide</i> for further details.
<code>courier</code>	Example font used for screen displays, prompts, and scripts.	Are you ready to continue? [Y]
courier bold	Example font used to indicate what the user enters in examples of command environments.	Login: root

Table 2 Command Syntax Conventions

Convention	Definition	Sample
vertical bars ()	Separate alternative, mutually exclusive elements	offset-list { in out } offset
square brackets ([])	Indicate optional elements	[no] offset-list { in out } offset
braces ({ })	Indicate a required choice	offset-list { in out } offset
braces within square brackets ([{ }])	Indicate a required choice within an optional element	[{ letter/number } Enter]
boldface	Indicates commands and keywords that are entered literally as shown	[no] offset-list { in out } offset
<i>italics</i>	Indicate arguments for which you supply values Note In contexts that do not allow italics, arguments are enclosed in angle brackets (< >).	offset-list { in out } offset

Table 3 Note, Timesaver, Tip, Caution, and Warning Conventions

Convention	Description
Note 	Means <i>reader take note</i> . Notes contain helpful suggestions or references to material not covered in the guide.
Timesaver 	Means <i>the described action saves time</i> . You can save time by performing the action described in the paragraph.
Caution 	Means <i>reader be careful</i> . In this situation, you might do something that could result in equipment damage or loss of data.
Warning 	Means <i>danger</i> . You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents. To see translated versions of warnings, refer to the <i>Regulatory Compliance and Safety Information</i> document that accompanied the device.

Obtaining Documentation

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

World Wide Web

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

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

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

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

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

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

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

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

<http://www.cisco.com>

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

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

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

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

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

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

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

Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

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



Supported Features

This chapter lists the features supported by the Cisco 6400 carrier-class broadband aggregator in Cisco IOS Release 12.2.(2)B. This chapter also identifies feature documentation that you can find on Cisco.com.

The topics addressed are:

- Conventions Used in This Chapter, page 1-2
- Node Route Processor Features, page 1-2
 - Access Protocols, page 1-3
 - Aggregation and Virtual Private Networks (VPNs), page 1-5
 - Configuration and Monitoring, page 1-7
 - Hardware Support, page 1-7
 - IP and Routing, page 1-8
 - IP QoS, page 1-10
 - Network Management, page 1-10
 - RADIUS/AAA, page 1-11
 - Scalability and Performance, page 1-12
 - Service Selection Gateway (NRP-SSG), page 1-13
 - Other Features and Feature Enhancements, page 1-16
- Node Switch Processor Features, page 1-17
 - ATM Connections, page 1-17
 - ATM Internetworking, page 1-18
 - ATM Per-Flow Queuing, page 1-18
 - ATM Traffic Classes, page 1-19
 - Configuration and Monitoring, page 1-20
 - Hardware Support, page 1-21
 - IP and Routing, page 1-22
 - Network Management, page 1-22
 - RADIUS/AAA, page 1-23
 - Scalability and Performance, page 1-23

- Signaling and Routing, page 1-23

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	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Miscellaneous Features • ATM Routed Bridge Encapsulation <p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Addressing and Services • Configuring DHCP
RFC 1577	<p><i>Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • 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
Integrated Routing and Bridging (IRB)	<p><i>DSL Architecture: Reliability Design Plan:</i></p> <ul style="list-style-type: none"> • DSL Network Architectures • Integrated Routing and Bridging (IRB)/RFC 1483 Bridging <p><i>Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Bridging
Multilink PPP (MLP)	<p><i>Cisco IOS Dial Technologies Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • PPP Configuration • Configuring Media-Independent PPP and Multilink PPP
Per-VC Traffic Shaping (NRP-1 and NRP-2SV only)	<p><i>Cisco 6400 Software Setup Guide:</i></p> <ul style="list-style-type: none"> • Basic NRP Configuration • Configuring PVC Traffic Shaping
PPP IPCP Subnet Negotiation	<p><i>Cisco IOS Dial Technologies Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • PPP Configuration • Configuring Asynchronous SLIP and PPP • Configuring Network-Layer Protocols over PPP and SLIP <p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Miscellaneous Features • IPCP Subnet Mask Support
PPP over ATM (PPPoA) terminated	<p><i>Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Configuring Broadband Access: PPP and Routed Bridge Encapsulation • Configuring PPP over ATM <p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Point-to-Point Protocol • Configuring PPPoA <p><i>PPPoA Baseline Architecture, white paper</i></p>
PPP over Ethernet (PPPoE) terminated	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Point-to-Point Protocol • Configuring PPPoE <p><i>Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Configuring Broadband Access: PPP and Routed Bridge Encapsulation <p><i>PPPoE Baseline Architecture for the Cisco 6400 UAC, white paper</i></p>

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

Feature	Documentation
PPP autosense (SNAP)	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Point-to-Point Protocol • Configuring PPP Autosense
Routed Bridge Encapsulation (RBE)	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Miscellaneous Features • ATM Routed Bridge Encapsulation <p><i>DSL Architecture: Reliability Design Plan:</i></p> <ul style="list-style-type: none"> • DSL Network Architectures • Routed Bridge Encapsulation (RBE)
RBE Subinterface Grouping	<i>ATM PVC Range and Routed Bridge Encapsulation Subinterface Grouping, 12.1(5)T feature module</i>
RBE unnumbered DHCP	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Miscellaneous Features • ATM Routed Bridge Encapsulation <p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Addressing and Services • Configuring DHCP
RBE with DHCP	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Miscellaneous Features • ATM Routed Bridge Encapsulation <p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Addressing and Services • Configuring DHCP
RBE with DHCP Option 82	<i>DHCP Option 82 Support for Routed Bridge Encapsulation, 12.2(2)T feature module</i>
RFC 1483 bridging	<p><i>DSL Architecture: Reliability Design Plan:</i></p> <ul style="list-style-type: none"> • DSL Network Architectures • Integrated Routing and Bridging (IRB)/RFC 1483 Bridging <p><i>Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Bridging <p><i>Cisco 6400 NRP Configuration and Troubleshooting, white paper</i></p> <p><i>Basic PVC Configuration Using Bridged RFC 1483, sample configuration</i></p>
RFC 1483 routing	<p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Routing Protocols <p><i>Cisco 6400 NRP Configuration and Troubleshooting, white paper</i></p>

Aggregation and Virtual Private Networks (VPNs)

Table 1-3 NRP Features—Aggregation and VPNs

Feature	Documentation
IP Overlapping Address Pools (OAP) (NRP-1 only)	<i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i> <ul style="list-style-type: none"> Miscellaneous Features IP Overlapping Address Pools
L2TP Multi-Hop	<i>Multihop VPDN</i> , 11.3(3)T feature module <i>Configuring L2TP Multihop to Perform Several Hops from the NAS to the LNS</i> , Sample Configuration
L2TP tunnel service authorization enhancement	<i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i> <ul style="list-style-type: none"> Layer 2 Tunnel Protocol Configuring L2TP Tunnel Service Authorization
L2TP tunnel sharing	<i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i> <ul style="list-style-type: none"> Layer 2 Tunnel Protocol Configuring L2TP Tunnel Sharing
L2TP tunnel switching	<i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i> <ul style="list-style-type: none"> Layer 2 Tunnel Protocol Configuring L2TP Tunnel Switching
MPLS Edge Label Switch Router (Edge LSR) (NRP-1 only)	<i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i> <ul style="list-style-type: none"> Multiprotocol Label Switching
MPLS Label Distribution Protocol (LDP)	<i>MPLS Label Distribution Protocol</i> , 12.2(2)T feature module
MPLS Label Switch Controller (LSC) for BPX (NRP-1 only)	<i>Cisco IOS Switching Services Configuration Guide, Release 12.2:</i> <ul style="list-style-type: none"> Multiprotocol Label Switching
MPLS VPNs	<i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i> <ul style="list-style-type: none"> Multiprotocol Label Switching Configuring MPLS Virtual Private Networks <i>Cisco IOS Switching Services Configuration Guide, Release 12.2:</i> <ul style="list-style-type: none"> Multiprotocol Label Switching

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

Feature	Documentation
PPPoA tunneled into L2TP	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Layer 2 Tunnel Protocol <p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Point-to-Point Protocol • Configuring PPPoA <p><i>Layer 2 Tunneling Protocol</i>, fact sheet</p>
PPPoE tunneled into L2TP	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Layer 2 Tunnel Protocol <p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Point-to-Point Protocol • Configuring PPPoE <p><i>Layer 2 Tunneling Protocol</i>, fact sheet</p>
Remote Access into MPLS VPN (NRP-1 only)	<p>Cisco Remote Access to MPLS VPN Solution 1.0 documentation</p> <p>DSL Access to MPLS VPN Integration</p> <p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Multiprotocol Label Switching • Configuring MPLS Virtual Private Networks <p><i>Cisco IOS Switching Services Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Multiprotocol Label Switching
RFC 1577	<p><i>Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Configuring ATM • Configuring Classical IP and ARP over ATM
VLAN (ISL) on NRP	<p><i>Cisco IOS Switching Services Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Virtual LANs • Configuring Routing Between VLANs with ISL Encapsulation
VLAN (802.1q) on GE (NRP-2 and NRP-2SV only)	<p><i>Cisco IOS Switching Services Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Virtual LANs • Configuring Routing Between VLANs with IEEE 802.1Q Encapsulation

Configuration and Monitoring

Table 1-4 NRP Features—Configuration and Monitoring

Feature	Documentation
ATM PVC Range Command	<i>ATM PVC Range and Routed Bridge Encapsulation Subinterface Grouping</i> , 12.1(5)T feature module
Per VC error display	<i>Cisco 6400 Command Reference</i> : <ul style="list-style-type: none"> Show Commands for the Cisco 6400 NRP show controllers atm 0/0/0

Hardware Support

Table 1-5 NRP Features—Hardware Support

Feature	Documentation
ATM (OC-3, OC-12, DS3) Interfaces	<i>Cisco 6400 Software Setup Guide</i> : <ul style="list-style-type: none"> Node Line Card Interface Configuration
FE Interface: 10/100 auto-negotiation, auto-sensing (NRP-1 only)	<i>Cisco IOS Interface Configuration Guide, Release 12.2</i> : <ul style="list-style-type: none"> Configuring LAN Interfaces Configuring Ethernet, Fast Ethernet, or Gigabit Ethernet Interfaces
GE Interface	<i>Gigabit Ethernet Port Adapter</i> , 12.1(4)E feature module
Network Management Ethernet (NME)	<i>Cisco 6400 Software Setup Guide</i> : <ul style="list-style-type: none"> Basic NSP Configuration Network Management Ethernet Interface Enabling NME Consolidation on the NRP
NRP 1+1 Redundancy (NRP-1 only)	<i>Cisco 6400 Software Setup Guide</i> : <ul style="list-style-type: none"> Redundancy and SONET APS Configuration NRP Redundancy

IP and Routing

Table 1-6 NRP Features—IP and Routing

Feature	Documentation
Address Resolution Protocol (ARP)	<p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Addressing and Services • Configuring IP Addressing • Configuring Address Resolution Methods
Border Gateway Protocol version 4 (BGP4)	<p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Routing Protocols • Configuring BGP
Enhanced Interior Gateway Routing Protocol (EIGRP)	<p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Routing Protocols • Configuring IP Enhanced IGRP
Generic routing encapsulation (GRE)	<p><i>Cisco IOS Interface Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Configuring Logical Interfaces • Configuring a Tunnel Interface
Internet Group Management Protocol (IGMP)	<p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Multicast • Configuring IP Multicast Routing • IGMP Features Configuration Task List
Internet Protocol (IP) forwarding	<p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Addressing and Services • Configuring IP Services
IP multicast	<p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Multicast <p><i>Internet Protocol (IP) Multicast Technology Overview, white paper</i></p>
Intermediate System-to-Intermediate System (IS-IS)	<p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Routing Protocols • Configuring Integrated IS-IS
Network Address Translation (NAT) support for NetMeeting Directory	<p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Addressing and Services • Configuring IP Addressing • Configuring Network Address Translation

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

Feature	Documentation
NetFlow for RFC1483 into MPLS VPN (NRP- 1 only)	<p><i>Cisco IOS Switching Services Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • NetFlow Switching <p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Multiprotocol Label Switching • Configuring MPLS Virtual Private Networks <p><i>Cisco IOS Technical Marketing NetFlow Deployment on Logical Interfaces, white paper</i></p>
Open Shortest Path First (OSPF)	<p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Routing Protocols • Configuring OSPF
PIM Dense Mode & Sparse Mode	<p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Multicast • Configuring IP Multicast Routing
Routing Information Protocol (RIP)/RIP v2	<p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Routing Protocols • Configuring Routing Information Protocol
Transmission Control Protocol (TCP)	<p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Overview
Telnet	<p><i>Cisco IOS Terminal Services Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Configuring Dial-In Terminal Services • Telnet and rlogin Configuration Task List
Trivial File Transfer Protocol (TFTP)	<p><i>Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • File Management • Configuring Basic File Transfer Services • Configuring a Router as a TFTP or RARP Server
Transparent Bridging	<p><i>Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Bridging • Configuring Transparent Bridging
User Datagram Protocol (UDP)	<p><i>Internetworking Technology Overview:</i></p> <ul style="list-style-type: none"> • Internet Protocols (IP) • Transmission Control Protocol (TCP) • User Datagram Protocol (UDP)

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

Feature	Documentation
Web Cache Coordination Protocol (WCCP) version 1	<i>Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2:</i> <ul style="list-style-type: none"> • System Management • Configuring Web Cache Services Using WCCP
WCCP (v2)	<i>Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2:</i> <ul style="list-style-type: none"> • System Management • Configuring Web Cache Services Using WCCP

IP QoS

Table 1-7 NRP Features—IP QoS

Feature	Documentation
IP QoS—Policing and Marking	<i>Cisco 6400 Release Notes</i> <ul style="list-style-type: none"> • IP QoS—Policing and Marking <i>Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2:</i> <ul style="list-style-type: none"> • Policing and Shaping

Network Management

Table 1-8 NRP Features—Network Management

Feature	Documentation
PPPoE session count MIB	<i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i> <ul style="list-style-type: none"> • Point-to-Point Protocol • Configuration Tasks • Configuring PPPoE Session Count MIB
SNMP (v1, v2, and v3)	<i>Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2:</i> <ul style="list-style-type: none"> • System Management • Configuring SNMP Support
SNMPv3 Proxy Forwarder (NRP-2 and NRP-2SV only)	<i>Cisco 6400 Software Setup Guide:</i> <ul style="list-style-type: none"> • SNMP, RMON, and Alarm Configuration • Using the NSP as the SNMPv3 Proxy Forwarder for the NRP-2

RADIUS/AAA

Table 1-9 NRP Features—RADIUS/AAA

Feature	Documentation
IETF Tunnel Attributes	<p><i>Cisco IOS Security Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Security Server Protocols • Configuring RADIUS • RADIUS Attributes
Password Authentication Protocol (PAP)/ Challenge Handshake Authentication Protocol (CHAP)	<p><i>Cisco IOS Security Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Authentication, Authorization, and Accounting (AAA) • Configuring Authentication • Non-AAA Authentication Methods • Enabling CHAP or PAP Authentication
Remote Authentication Dial-In User Service (RADIUS)	<p><i>Cisco IOS Security Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Security Server Protocols • Configuring RADIUS
RADIUS Attribute 8 (Framed-IP-Address) in Access Requests (also known as “IP Hint” or “Sticky IP”)	<p><i>RADIUS Attribute 8 (Framed-IP-Address) in Access Requests, 12.1(5)T feature module</i></p>
Terminal Access Controller Access Control System Plus (TACACS+) (admin login only)	<p><i>Cisco IOS Security Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Security Server Protocols • Configuring TACACS+
VPI/VCI in RADIUS Request and RADIUS Accounting for PPPoA	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Miscellaneous Features • RADIUS VC Logging
VPI/VCI in RADIUS Request and RADIUS Accounting for PPPoE	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Miscellaneous Features • RADIUS VC Logging

Scalability and Performance

Table 1-10 NRP Features—Scalability and Performance

Feature	Documentation
GRE Cisco express forwarding (CEF)	<p><i>Cisco IOS Switching Services Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Cisco IOS Switching Paths <p><i>Cisco IOS Interface Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Configuring Logical Interfaces • Configuring a Tunnel Interface
LAC CEF switching	<p><i>Cisco IOS Switching Services Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Cisco IOS Switching Paths <p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Layer 2 Tunnel Protocol • Configuring L2TP • Configuring VPDN on the LAC <p><i>Layer 2 Tunneling Protocol, fact sheet</i></p>
L2TP sessions per tunnel limiting	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Layer 2 Tunnel Protocol • Configuring L2TP • Sessions per Tunnel Limiting
NAT CEF switching	<p><i>Cisco IOS Switching Services Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Cisco IOS Switching Paths <p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • IP Addressing and Services • Configuring IP Addressing • Configuring Network Address Translation
Per VC buffer management	<p><i>Cisco 6400 Software Setup Guide:</i></p> <ul style="list-style-type: none"> • Basic NRP Configuration • NRP-1 Configuration • Segmentation and Reassembly Buffer Management
PPPoA CEF	<p><i>Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Configuring Broadband Access: PPP and Routed Bridge Encapsulation • Configuring PPP over ATM <p><i>Cisco IOS Switching Services Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Cisco IOS Switching Paths

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

Feature	Documentation
PPPoE Fast Switching for Multicast	<p><i>Cisco IOS Dial Technologies Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • PPP Configuration • Configuring Asynchronous SLIP and PPP • Enabling Fast Switching
PPPoE Session Limit (per ATM VC)	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Point-to-Point Protocol • Configuration Tasks • Configuring PPPoE Session Limit
RBE CEF	<p><i>Cisco IOS Switching Services Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> • Cisco IOS Switching Paths <p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Miscellaneous Features • ATM Routed Bridge Encapsulation <p><i>DSL Architecture: Reliability Design Plan:</i></p> <ul style="list-style-type: none"> • DSL Network Architectures • Routed Bridge Encapsulation (RBE)

Service Selection Gateway (NRP-SSG)

Table 1-11 NRP Features—SSG

Feature	Documentation
PPP Termination and Aggregation Multi-Domain (PTA-MD)	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Service Selection Gateway • Overview • Benefits • Multiple Traffic-Type Support • PPP Termination Aggregation (PTA) and PTA Multi-Domain (PTA-MD)
RADIUS Interim Accounting	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Service Selection Gateway • Configuring Features • Configuring RADIUS Interim Accounting
SSG AAA Server Group Support for Proxy Services	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Service Selection Gateway • Configuring Features • Configuring AAA Server Group Support for Proxy Services

Table 1-11 NRP Features—SSG (continued)

Feature	Documentation
SSG Automatic Service Logon	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Service Selection Gateway • Configuring RADIUS Profiles • User Profiles • Auto Service
SSG CEF Switching	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Service Selection Gateway • Configuring Features • Configuring Cisco Express Forwarding
SSG Default Network	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Service Selection Gateway • Configuring Features • Configuring a Default Network
SSG DNS Fault Tolerance	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Service Selection Gateway • Configuring RADIUS Profiles • Service Profiles • DNS Server Address
SSG enable (default is disabled)	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Service Selection Gateway • Configuring Features • Enabling SSG
SSG full username RADIUS attribute	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Service Selection Gateway • Configuring RADIUS Profiles • Service Profiles • Full Username Attribute
SSG Host Key	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> • Service Selection Gateway • Configuring Features • Configuring Host Key
SSG Cisco IOS NAT support	<p><i>Cisco 6400 Command Reference:</i></p> <ul style="list-style-type: none"> • SSG Commands for the Cisco 6400 NRP • debug ssg data-nat

Table 1-11 NRP Features—SSG (continued)

Feature	Documentation
SSG Local Forwarding	<i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i> <ul style="list-style-type: none"> • Service Selection Gateway • Configuring Features • Configuring Local Forwarding
SSG Open Garden	<i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i> <ul style="list-style-type: none"> • Service Selection Gateway • Configuring Features • Configuring an Open Garden
SSG Passthrough and Proxy Service	<i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i> <ul style="list-style-type: none"> • Service Selection Gateway • Configuring RADIUS Profiles • Service Profiles • Type of Service
SSG Sequential and Concurrent Service	<i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i> <ul style="list-style-type: none"> • Service Selection Gateway • Configuring RADIUS Profiles • Service Profiles • Service Mode
SSG Service Defined Cookie	<i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i> <ul style="list-style-type: none"> • Service Selection Gateway • Configuring RADIUS Profiles • Service Profiles • Service-Defined Cookie
SSG single host logon	<i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i> <ul style="list-style-type: none"> • Service Selection Gateway • Overview • Benefits • SSG Single Host Logon
SSG TCP Redirect - Logon (Previously called “HTTP Redirect”)	<i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i> <ul style="list-style-type: none"> • Service Selection Gateway • Configuring Features • Configuring TCP Redirect - Logon

Table 1-11 NRP Features—SSG (continued)

Feature	Documentation
SSG with GRE	<p><i>Cisco IOS Interface Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> Configuring Logical Interfaces Configuring a Tunnel Interface <p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> Service Selection Gateway
SSG with Multicast	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> Service Selection Gateway Configuring Features Configuring Multicast <p><i>Cisco IOS IP Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> IP Multicast
SSG with L2TP Service Type	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> Service Selection Gateway Configuring Features Configuring SSG with L2TP Service Type
VPI/VCI Static binding to a Service Profile	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> Service Selection Gateway Configuring Features Configuring VPI/VCI Indexing to Service Profile
WebSelection	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> Service Selection Gateway <p>Cisco Subscriber Edge Services Manager documentation</p> <p>Cisco Service Selection Dashboard documentation</p>

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)	<p><i>Cisco 6400 Software Setup Guide:</i></p> <ul style="list-style-type: none"> Basic NRP Configuration NRP-1 Configuration Segmentation and Reassembly Buffer Management
Session Scalability Enhancements	<p><i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i></p> <ul style="list-style-type: none"> Session and Tunnel Scalability

Node Switch Processor Features

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

ATM Connections

Table 1-13 NSP Features—ATM Connections

Feature	Documentation
F4 and F5 Operation, administration, and maintenance (OAM) cell segment and end-to-end flows	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Operation, Administration, and Maintenance
Hierarchical virtual private (VP) tunnels	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Virtual Connections Configuring VP Tunnels Configuring a Hierarchical VP Tunnel for Multiple Service Categories
Logical multicast support (up to 254 leaves per output port, per point-to-multipoint virtual circuits [VCs])	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Virtual Connections Configuring Point-to-Multipoint PVC Connections
Multipoint-to-point User-Network Interface (UNI) signaling	<i>Cisco 6400 Software Setup Guide:</i> <ul style="list-style-type: none"> Node Line Card Interface Configuration ATM Interface Types User-Network Interfaces
Point-to-Point and Point-to-Multipoint VCs	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Virtual Connections
Permanent virtual circuit (PVC), Soft PVC, Soft permanent virtual path (PVP), and switched virtual circuit (SVC)	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Virtual Connections
Soft virtual channel connections (VCCs) and virtual path connections (VPCs)	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Virtual Connections
VC Merge	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Tag Switching Configuring VC Merge
VP and VC switching	<i>Cisco 6400 Software Setup Guide:</i> <ul style="list-style-type: none"> Basic NSP Configuration Internal Cross-Connections

Table 1-13 NSP Features—ATM Connections (continued)

Feature	Documentation
VP multiplexing	<i>Understanding VP Tunnels and VP Switching</i> , tech note
VP tunneling	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Virtual Connections Configuring VP Tunnels

ATM Internetworking

Table 1-14 NSP Features—ATM Internetworking

Feature	Documentation
LAN Emulation Server (LES) and LAN Emulation Configuration Server (LECS)	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring LAN Emulation
RFC 1577 (Classical IP over ATM) ATM Address Resolution Protocol (ARP) server/client	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring IP over ATM Configuring Classical IP over ATM

ATM Per-Flow Queuing

Table 1-15 NSP Features—ATM Per-Flow Queuing

Feature	Documentation
Dual leaky bucket policing (ITU-T I.371 and ATM Forum UNI specifications)	<i>Guide to ATM Technology:</i> <ul style="list-style-type: none"> Traffic and Resource Management UPC—Traffic Policing at a Network Boundary <i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Resource Management Processor Feature Card Functionality¹
Intelligent early packet discard (EPD)	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Resource Management Configuring Physical Interfaces Configuring the Interface Queue Thresholds per Service Category <i>ATM and Layer 3 Switch Router Command Reference:</i> <ul style="list-style-type: none"> ATM Commands atm output-threshold <i>LightStream 1010 Switch Architecture and Traffic Management</i> , white paper

Table 1-15 NSP Features—ATM Per-Flow Queuing (continued)

Feature	Documentation
Intelligent partial (tail) packet discard	<p><i>ATM Switch Router Software Configuration Guide:</i></p> <ul style="list-style-type: none"> Configuring Resource Management Configuring Physical Interfaces Configuring the Interface Queue Thresholds per Service Category <p><i>LightStream 1010 Switch Architecture and Traffic Management</i>, white paper</p>
Multiple, weighted (dynamic) thresholds for selective packet marking and discard	<p><i>ATM Switch Router Software Configuration Guide:</i></p> <ul style="list-style-type: none"> Configuring Resource Management Processor Feature Card Functionality¹
Per-VC or per-VP output queuing	<p><i>ATM Switch Router Software Configuration Guide:</i></p> <ul style="list-style-type: none"> Configuring Resource Management Processor Feature Card Functionality¹
Strict priority, rate, or weighted round robin scheduling algorithms	<p><i>ATM Switch Router Software Configuration Guide:</i></p> <ul style="list-style-type: none"> Configuring Resource Management Configuring Physical Interfaces Configuring the Scheduler and Service Class

1. The NSP uses the FC-PFQ feature card.

ATM Traffic Classes

Table 1-16 NSP Features—ATM Traffic Classes

Feature	Documentation
Available bit rate (ABR) (EFCI + RR) + minimum cell rate (MCR)	<p><i>ATM Switch Router Software Configuration Guide:</i></p> <ul style="list-style-type: none"> Configuring Resource Management Configuring Physical Interfaces Configuring the Interface Queue Thresholds per Service Category
ABR connection support for non-zero MCR	<p><i>ATM Switch Router Software Configuration Guide:</i></p> <ul style="list-style-type: none"> Configuring Resource Management Configuring Physical Interfaces Configuring the Interface Queue Thresholds per Service Category¹
Constant bit rate (CBR)	<p><i>ATM Switch Router Software Configuration Guide:</i></p> <ul style="list-style-type: none"> Configuring Resource Management Configuring Global Resource Management
Per-VC or per-VP CBR traffic shaping	<p><i>ATM Switch Router Software Configuration Guide:</i></p> <ul style="list-style-type: none"> Configuring Resource Management Configuring Global Resource Management¹

Table 1-16 NSP Features—ATM Traffic Classes (continued)

Feature	Documentation
Shaped CBR VP tunnels (up to 128)	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Resource Management Configuring Global Resource Management¹
Substitution of other service categories in shaped VP tunnels	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Resource Management Configuring Physical and Logical Interface Parameters Configuring Interface Service Category Support
Unspecified bit rate (UBR)	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Resource Management Configuring Global Resource Management¹
UBR + MCR	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Resource Management Configuring Global Resource Management Configuring the Connection Traffic Table CTT Supported Features
Variable bit rate-non-real time (VBR-nrt)	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Resource Management Configuring Global Resource Management¹
VBR-real time (VBR-rt)	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Resource Management Configuring Global Resource Management¹

1. The NSP uses the FC-PFQ feature card.

Configuration and Monitoring

Table 1-17 NSP Features—Configuration and Monitoring

Feature	Documentation
ATM access lists on Interim Local Management Interface (ILMI) registration	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Using Access Control Configuring Per-Interface Address Registration with Optional Access Filters

Table 1-17 NSP Features—Configuration and Monitoring (continued)

Feature	Documentation
PCMCIA Disk Mirroring	<i>Cisco 6400 Software Setup Guide:</i> <ul style="list-style-type: none"> • Redundancy and SONET APS Configuration • NSP Redundancy • PCMCIA Disk Mirroring
Per-VC or per-VP nondisruptive port snooping	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> • Configuring Virtual Connections • Configuring Interface and Connection Snooping • Configuring Per-Connection Snooping

Hardware Support

Table 1-18 NSP Features—Hardware Support

Feature	Documentation
1+1 Slot Redundancy (EHSA)	<i>Cisco 6400 Software Setup Guide:</i> <ul style="list-style-type: none"> • Redundancy and SONET APS Configuration
Network Management Ethernet (NME)	<i>Cisco 6400 Software Setup Guide:</i> <ul style="list-style-type: none"> • Basic NSP Configuration • Network Management Ethernet Interface
NRP-2 support	<i>Cisco 6400 Software Setup Guide:</i> <ul style="list-style-type: none"> • Basic NSP Configuration • NRP-2 Support
NSP 1+1 Redundancy	<i>Cisco 6400 Software Setup Guide:</i> <ul style="list-style-type: none"> • Redundancy and SONET APS Configuration • NSP Redundancy
Synchronous Optical Network (SONET) automatic protection switching (APS) support	<i>Cisco 6400 Software Setup Guide:</i> <ul style="list-style-type: none"> • Redundancy and SONET APS Configuration • SONET APS for NLC Port Redundancy
Stratum 3/BITS	<i>Cisco 6400 Software Setup Guide:</i> <ul style="list-style-type: none"> • Basic NSP Configuration • Network Clocking • Configuring Building Integrated Timing Supply Network Clocking
Telco alarms	<i>Cisco 6400 Software Setup Guide:</i> <ul style="list-style-type: none"> • SNMP, RMON, and Alarm Configuration • Alarms

IP and Routing

Table 1-19 NSP Features—IP and Routing

Feature	Documentation
Dynamic Host Configuration Protocol (DHCP) client support	<i>Cisco IOS IP Configuration Guide, Release 12.2:</i> <ul style="list-style-type: none"> IP Addressing and Services Configuring DHCP
Internet Protocol (IP)	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring IP over ATM
Network Time Protocol (NTP)	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring System Management Functions Configuring the Network Time Protocol
Telnet	<i>Cisco IOS Terminal Services Configuration Guide, Release 12.2:</i> <ul style="list-style-type: none"> Configuring Dial-In Terminal Services Telnet and rlogin Configuration Task List

Network Management

Table 1-20 NSP Features—Network Management

Feature	Documentation
ATM accounting enhancements	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring ATM Accounting and ATM RMON
ATM Accounting Management Information Base (MIB)	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring ATM Accounting and ATM RMON
ATM remote monitoring (RMON) MIB	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring ATM Accounting and ATM RMON
ATM SNMP trap and OAM enhancements	<i>Cisco 6400 Feature Guide—Release 12.2.(2)B:</i> <ul style="list-style-type: none"> Miscellaneous Features ATM SNMP Trap and OAM Enhancements
Signaling diagnostics and MIB	<i>ATM Switch Router Software Configuration Guide:</i> <ul style="list-style-type: none"> Configuring Signalling Features Configuring Signalling Diagnostics Tables
Simple Network Management Protocol (SNMP)	<i>Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2:</i> <ul style="list-style-type: none"> System Management Configuring SNMP Support
Web Console	<i>Cisco 6400 Software Setup Guide:</i> <ul style="list-style-type: none"> Web Console

RADIUS/AAA

Table 1-21 NSP Features—RADIUS/AAA

Feature	Documentation
Terminal Access Controller Access Control System Plus (TACACS+) (admin login only)	<p><i>ATM Switch Router Software Configuration Guide:</i></p> <ul style="list-style-type: none"> Configuring System Management Functions Configuring TACACS <p><i>Cisco IOS Security Configuration Guide, Release 12.2:</i></p> <ul style="list-style-type: none"> Security Server Protocols Configuring TACACS+

Scalability and Performance

Table 1-22 NSP Features—Scalability and Performance

Feature	Documentation
Capability to view used/unused Input Translation Table (ITT) blocks	<p><i>Cisco 6400 Software Setup Guide:</i></p> <ul style="list-style-type: none"> Optimizing the Number of Virtual Connections on the Cisco 6400 Displaying ITT Allocation
Fragmentation minimization	<p><i>Cisco 6400 Software Setup Guide:</i></p> <ul style="list-style-type: none"> Optimizing the Number of Virtual Connections on the Cisco 6400
ITT block shrinking	<p><i>Cisco 6400 Software Setup Guide:</i></p> <ul style="list-style-type: none"> Optimizing the Number of Virtual Connections on the Cisco 6400

Signaling and Routing

Table 1-23 NSP Features—Signaling and Routing

Feature	Documentation
ATM Network Service Access Point (NSAP) and left-justified E.164 address support	<p><i>ATM Switch Router Software Configuration Guide:</i></p> <ul style="list-style-type: none"> Configuring Signalling Features Configuring E.164 Addresses <p><i>ATM and Layer 3 Switch Router Command Reference:</i></p> <ul style="list-style-type: none"> A Commands aesa embedded-number left-justified
Closed user groups (CUGs) for ATM VPNs	<p><i>ATM Switch Router Software Configuration Guide:</i></p> <ul style="list-style-type: none"> Configuring Signalling Features Configuring Closed User Group Signalling

Table 1-23 NSP Features—Signaling and Routing (continued)

Feature	Documentation
E.164 address translation and autoconversion	<p><i>ATM Switch Router Software Configuration Guide:</i></p> <ul style="list-style-type: none"> • Configuring Signalling Features • Configuring E.164 Addresses
Hierarchical Private Network Node Interface (PNNI)	<p><i>ATM Switch Router Software Configuration Guide:</i></p> <ul style="list-style-type: none"> • Configuring ATM Routing and PNNI • Basic PNNI Configuration <p><i>Guide to ATM Technology:</i></p> <ul style="list-style-type: none"> • ATM Routing with IISP and PNNI • PNNI Overview • Hierarchical PNNI
Interim-Interswitch Signaling Protocol (IISP)	<p><i>Cisco 6400 Software Setup Guide:</i></p> <ul style="list-style-type: none"> • Node Line Card Interface Configuration • ATM Interface Types • Interim Interswitch Signaling Protocol Interfaces <p><i>Guide to ATM Technology:</i></p> <ul style="list-style-type: none"> • ATM Routing with IISP and PNNI • Static Routing with IISP
ILMI 4.0	<p><i>ATM Switch Router Software Configuration Guide</i></p> <ul style="list-style-type: none"> • Configuring ILMI
VPI/VCI range support in ILMI 4.0	<p><i>ATM Switch Router Software Configuration Guide:</i></p> <ul style="list-style-type: none"> • Configuring Virtual Connections • Configuring a VPI/VCI Range for SVPs and SVCs
UNI 3.0, UNI 3.1, and UNI 4.0	<p><i>Cisco 6400 Software Setup Guide:</i></p> <ul style="list-style-type: none"> • Node Line Card Interface Configuration • ATM Interface Types • User-Network Interfaces



Layer 2 Tunnel Protocol

Overview

This chapter describes the Layer 2 tunnel protocol (L2TP) features supported in Cisco IOS Release 12.2(2)B.

Defined by RFC 2661, L2TP is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). For a description, benefits, restrictions, and configuration information for L2TP, see the “Configuring Virtual Private Networks” chapter in the “Virtual Templates, Profiles, and Networks” part of the *Cisco IOS Dial Technologies Configuration Guide, Release 12.2*.

Restrictions

L2TP Tunnel Service Authorization

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

L2TP Tunnel Switching

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 Scalability

The total number of precloned interfaces must not exceed 3000 on the Cisco 6400 NRP.

L2TP Scalability Prerequisites

Cisco Express Forwarding

To support over 1000 sessions, you must enable Cisco Express Forwarding (CEF) with the `ip cef` global configuration command. For more information on CEF, see the “Cisco Express Forwarding” chapter in the “Cisco IOS Switching Paths” part of the *Cisco IOS Switching Services Configuration Guide*.

Recommended Memory

Cisco recommends at least 128 MB of DRAM on the Cisco 6400 NRP while using these feature enhancements.

Configuring L2TP

Configuring L2TP involves the following tasks:

- Configuring VPDN on the LAC
- Configuring VPDN on the LNS
- Tunnel Service Authorization
- Sessions per Tunnel Limiting
- Tunnel Sharing
- Tunnel Switching

Configuring VPDN on the LAC

The L2TP access concentrator (LAC) is a device that is typically (although not always) located at a service provider's POP. Initial configuration and ongoing management is done by the service provider. Enter the following commands to enable VPDN on a LAC by using L2TP beginning in global configuration mode:

	Command	Purpose
Step 1	<code>vpdn enable</code>	Enables VPDN and informs the router to look for tunnel definitions from an LNS.
Step 2	<code>vpdn group <i>group-number</i></code>	Defines a local group number identifier for which other VPDN variables can be assigned. Valid group numbers range between 1 and 3000.
Step 3	<code>request dialin [<i>l2f</i> <i>l2tp</i>] ip <i>ip-address</i> {<i>domain domain-name</i> <i>dnis dialed-number</i>}</code>	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.

Configuring VPDN on the LNS

The L2TP network server (LNS) is the termination point for an L2TP tunnel. The LNS initiates outgoing calls and receives incoming calls from the LAC. To configure the LNS to initiate and receive calls, enter the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>vpdn enable</code>	Enables VPDN and informs the router to look for tunnel definitions from an LNS.
Step 2	<code>vpdn group group-number</code>	Defines a local group number identifier for which other VPDN variables can be assigned. Valid group numbers range between 1 and 3000.
Step 3	<code>accept dialin [l2f l2tp any] virtual-template virtual-template number remote remote-peer-name</code>	Allows the LNS to accept an open tunnel request from the specified remote peer, define the Layer 2 protocol to use for the tunnel, and identify the virtual template to use for cloning virtual access interfaces.

At this point, 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. The virtual template 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. Enter the following commands to create and configure a virtual template interface beginning in global configuration mode:

	Command	Purpose
Step 1	<code>interface virtual-template number</code>	Creates a virtual template interface and enters interface configuration mode.
Step 2	<code>ip unnumbered ethernet 0</code>	Enables IP without assigning a specific IP address on the LAN.
Step 3	<code>encapsulation ppp</code>	Enables PPP encapsulation on the virtual template interface, which will be applied to virtual access interfaces.
Step 4	<code>ppp authentication pap chap</code>	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 *Dial Solutions Configuration Guide*.

Refer to the “Important Notes” section of the release notes to learn about scaling and enhancing VPDN and L2TP features.

Tunnel Service Authorization



Note

Static tunnel service authorization does not support SVCs.

The tunnel service authorization enhancements enable the L2TP access concentrator (LAC) to conduct static or dynamic tunnel service authorization. A static domain name can be configured on the ATM PVC port 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 now 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.

Configuring a Static Domain Name

You can configure the static domain name on the PVC or on the VC class.

To configure the static domain name 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.
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.

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.

	Command	Purpose
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 VC class to all VCs on the ATM interface or subinterface.

Verifying the Static Domain Name

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

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.

Verifying Domain Preauthorization

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

Configuring the LAC to Communicate with the RADIUS Server

To enable the LAC to communicate properly with the RADIUS server for tunnel service authorization, enter the following commands 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.

Verifying LAC and RADIUS Server Communication

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.

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
<code>nas-port:ip-address:slot/subslot/port/vpi.vci</code>	Configures the NAS port username for domain preauthorization.
<code>Password = "cisco"</code>	Sets the fixed password.
<code>User-Service-Type = Outbound-User</code>	Configures the service-type as outbound.
<code>Cisco-AVpair = "vpdn:vpn-domain-list=domain1, domain2,..."</code>	Specifies the domains accessible to the user.

Syntax Description

<i>ip-address</i>	Management IP address of the NSP.
<i>slot/subslot/port</i>	Specify ATM interface.
<i>vpi.vci</i>	VPI and VCI values for the PVC.
<i>domain</i>	Domain to configure as accessible to the user.

Verifying the RADIUS User Profile for Domain Preauthorization

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

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
<code>domain Password "cisco"</code>	Sets the fixed password.
<code>User-Service-Type = Outbound-User</code>	Configures the service-type as outbound.
<code>Cisco-AVpair = "vpdn:tunnel-id=name"</code>	Specifies the name of the tunnel that must match the LNS's VPDN terminate-from hostname.
<code>Cisco-AVpair = "vpdn:l2tp-tunnel-password=secret"</code>	Specifies the secret (password) for L2TP tunnel authentication.
<code>Cisco-AVpair = "vpdn:tunnel-type=l2tp"</code>	Specifies Layer 2 Tunnel Protocol.
<code>Cisco-AVpair = "vpdn:ip-addresses=ip-address"</code>	Specifies IP address of LNS.

Syntax Description

<i>domain</i>	Client-supplied domain.
<i>name</i>	Name of the tunnel that must match the LNS's VPDN terminate-from hostname statement.
<i>secret</i>	Secret (password) used for L2TP tunnel authentication.
<i>ip-address</i>	IP address of LNS.

Verifying the RADIUS Service Profile for Tunnel Service Authorization

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

L2TP Tunnel Service Authorization Example

This section contains the following examples:

- Static Domain Name Configuration on a PVC Example
- Static Domain Name Configuration on a VC Class Example
- Domain Preauthorization Configuration on the LAC Example
- Domain Preauthorization RADIUS User Profile Example
- Tunnel Service Authorization Configuration on the LAC Example
- Tunnel Service Authorization RADIUS Service Profile Example

Static Domain Name Configuration on a PVC Example

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, while 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 aal5cisco ppp Virtual-Template1
    vpn service net1.com
  !
  pvc 30/34
    encapsulation aal5cisco ppp Virtual-Template1
    vpn service net2.com
  !
```

Static Domain Name Configuration on a VC Class Example

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 aal5cisco ppp 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
  !
```

Domain Preauthorization Configuration on the LAC Example

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
!
```

Domain Preauthorization RADIUS User Profile Example

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
    }
  }
}
```

Tunnel Service Authorization Configuration on the LAC Example

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
!
```

Tunnel Service Authorization RADIUS Service Profile Example

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
}
}
}

```

Sessions per Tunnel Limiting

This feature enables the **initiate-to** command to limit the number of sessions per L2TP tunnel.

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 <i>number</i>	Selects the VPDN group.
Step 2	Router(config- <i>vpdn</i>)# request-dialin	Enables the LAC to request L2TP tunnels to the LNS. Enters VPDN request-dialin group mode.
Step 3	Router(config- <i>vpdn-req-in</i>)# protocol l2tp	Specifies the Layer 2 Tunnel Protocol.
Step 4	Router(config- <i>vpdn-req-in</i>)# multihop <i>hostname</i> <i>ingress-tunnel-name</i> or Router(config- <i>vpdn-req-in</i>)# domain <i>domain-name</i> or Router(config- <i>vpdn-req-in</i>)# dnis <i>dnis-number</i>	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- <i>vpdn-req-in</i>)# exit	Returns to VPDN group mode.
Step 6	Router(config- <i>vpdn</i>)# initiate-to ip <i>ip-address</i> limit <i>limit-number</i> [priority <i>priority-number</i>]	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

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
...
```

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

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

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

Syntax Description

<i>address</i>		IP address of the LNS.
<i><delimiter></i>	, (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, 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

<i>limit</i>	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

The following example shows a tunnel service authorization RADIUS service profile, along with the session limiting entry. IP addresses 10.1.1.1 and 10.2.2.2 are assigned priority 1, while 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 authorized with different domains to share the same tunnel.

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	<code>Router(config)# vpdn-group number</code>	Selects the VPDN group.
Step 2	<code>Router(config-vpdn)# request-dialin</code>	Enables the LAC to request L2TP tunnels to the LNS. Enters VPDN request-dialin group mode.
Step 3	<code>Router(config-vpdn-req-in)# protocol l2tp</code>	Specifies the Layer 2 Tunnel Protocol.
Step 4	<code>Router(config-vpdn-req-in)# multihop hostname ingress-tunnel-name</code> or <code>Router(config-vpdn-req-in)# domain domain-name</code> or <code>Router(config-vpdn-req-in)# dnis dnis-number</code>	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. Note Repeat Step 4 to enter all keys chosen for tunnel sharing.
Step 5	<code>Router(config-vpdn-req-in)# exit</code>	Returns to VPDN group mode.
Step 6	<code>Router(config-vpdn)# initiate-to ip ip-address [priority priority-number]</code>	Specifies the LNS IP address. Optionally specifies the priority of the IP address (1 is highest).
Step 7	<code>Router(config-vpdn)# tunnel share</code>	Enables tunnel sharing among the keys entered in Step 4.

Example

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.

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

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"
```

Syntax Description

<i>group-name</i>	Group to which the service belongs.
-------------------	-------------------------------------

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

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



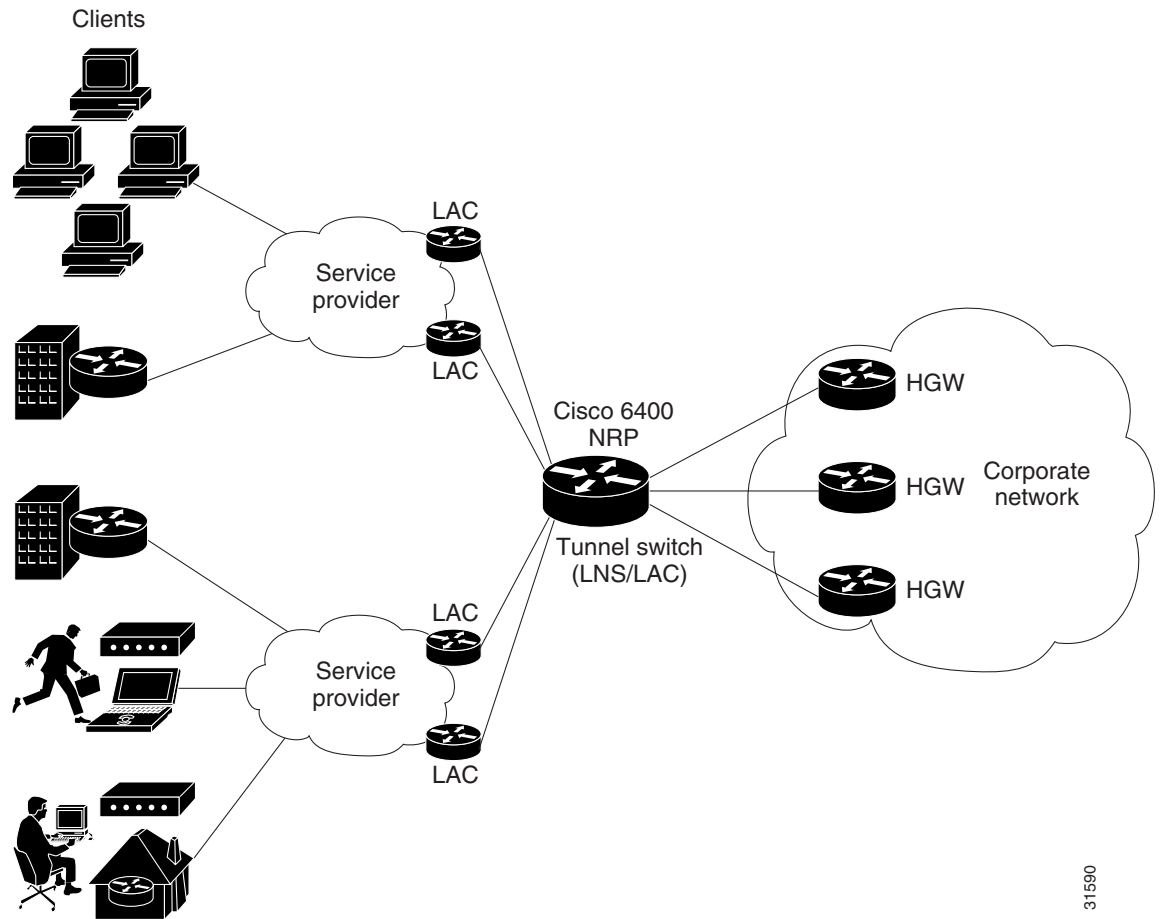
Note

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.

The L2TP Tunnel Switching feature enables the Cisco 6400 node route processor (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 LNSes.

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



See the following procedures to configure the L2TP Tunnel Switching feature. The listed tasks are required to configure the L2TP tunnel switch.

- Enabling VPDN and Multihop Functionality
- Terminating the Tunnel from the LAC
- Mapping the Ingress Tunnel Name to an LNS
- 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.

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 beginning 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.

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 configured on the LAC.
Step 2	Router(config)# username local-name password secret	Configures the secret (password). Must match <i>secret</i> in Step 1.
Step 3	Router(config)# vpdn-group number	Selects the VPDN group.
Step 4	Router(config- <i>vpdn</i>)# accept-dialin	Accepts incoming L2TP tunnel connections. Enters VPDN <i>accept-dialin</i> group mode.
Step 5	Router(config- <i>vpdn-acc-in</i>)# protocol l2tp	Specifies the Layer 2 Tunnel Protocol.
Step 6	Router(config- <i>vpdn-acc-in</i>)# virtual-template number	Specifies the virtual template interface to use to clone the new virtual access interface.
Step 7	Router(config- <i>vpdn-acc-in</i>)# exit	Returns to VPDN group mode.
Step 8	Router(config- <i>vpdn</i>)# terminate-from hostname remote-hostname	Specifies the host name of the remote LAC that will be required when accepting a VPDN tunnel. Must match <i>remote-hostname</i> in Step 1.
Step 9	Router(config- <i>vpdn</i>)# local name local-name	Specifies the local host name of the tunnel. Must match <i>local-name</i> 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.

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

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 <i>multihop-hostname</i> [<i>domain</i>]	Specifies a search by the configured ingress tunnel name. Optionally specifies to search by domain or DNIS if the first search type fails.

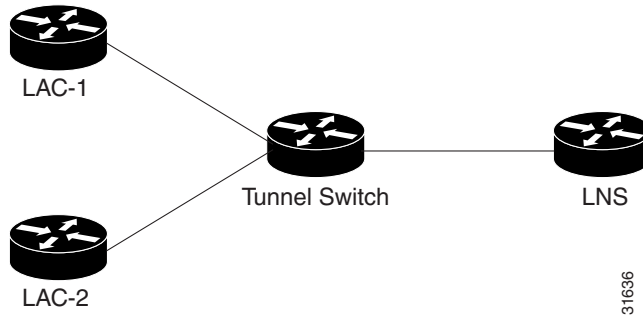
Verifying VPDN Tunnel Authorization Searches by Ingress Tunnel Name

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.

L2TP Tunnel Switching Example

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:

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

LAC-1 Configuration Example

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
!

```

LAC-2 Configuration Example

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
!
```

L2TP Tunnel Switch Configuration Example

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
!
```

LNS Configuration Example

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
!

```

Monitoring and Troubleshooting VPDN and L2TP

To troubleshoot VPDN and L2TP, enter the privileged EXEC command **debug vpdn**. For sample output of **debug vpdn**, see the “Debug Examples” section in the *Layer 2 Tunnel Protocol* feature module.

You can also enter the privileged EXEC command **show vpdn tunnel all**, which contains information for on L2TP scalability. The scalability related fields are described in Table 2-1.

```

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 2-1 show vpdn tunnel all *Field Descriptions*

Field as appears in 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.

Table 2-1 show vpdn tunnel all *Field Descriptions*

Field as appears in Example	Description
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.

Table 2-2 describes privileged EXEC commands that help you monitor and maintain VPDNs that use L2TP tunnels.

Table 2-2 VPDN Monitoring and Maintaining Commands

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

Troubleshooting components in VPDN is not always straightforward because there are multiple technologies and OSI layers involved. Table 2-3 describes EXEC commands that will help you isolate and identify problems on VPDNs that use L2TP tunnels:

Table 2-3 VPDN Troubleshooting Commands

Command	Purpose
<code>clear vpdn tunnel [l2f [nas-name hgw-name] l2tp [remote-name local-name]]</code>	Shuts down a specific tunnel and all the sessions within the tunnel.
<code>debug ppp negotiation</code>	Displays information about packets transmitted during PPP start-up and detailed PPP negotiation options.
<code>debug ppp chap</code>	Displays CHAP packet exchanges.
<code>debug vpdn event [protocol flow-control]</code>	Displays VPDN errors and basic events within the protocol (such as L2TP, L2F, PPTP) and errors associated with flow control. Flow control is only possible if you are using L2TP and the remote peer “receive window” is configured for a value greater than zero.
<code>debug vpdn packet [control data] [detail]</code>	Displays protocol-specific packet header information, such as sequence numbers if present, such as flags and length.

Table 2-3 VPDN Troubleshooting Commands

Command	Purpose
<code>show interface virtual access <i>number</i></code>	Displays information about the virtual access interface, LCP, protocol states, and interface statistics. The status of the virtual access interface should be: "Virtual-Access3 is up, line protocol is up"
<code>show vpdn session [all [interface tunnel username] packets sequence state timers window]</code>	Displays VPDN session information including interface, tunnel, username, packets, status, and window statistics.
<code>show vpdn tunnel [all [id local-name remote-name] packets state summary transport]</code>	Displays VPDN tunnel information including tunnel protocol, id, local and remote tunnel names, packets sent and received, tunnel, and transport status.



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(2)B.

This chapter only includes information that is specific to the Cisco 6400 and supplements the MPLS overview, configuration, verification, monitoring, and troubleshooting information in the *Cisco IOS Switching Services Configuration Guide* and the *ATM Switch Router Software Configuration Guide* (where MPLS is called “Tag Switching”).

This chapter includes the following sections:

- Restrictions, page 3-1
- Prerequisites, page 3-1
- MPLS Edge Label Switch Router, page 3-2
- MPLS Virtual Private Networks, page 3-7

For a complete list of MPLS and MPLS-related features supported in Cisco IOS Release 12.2(2)B, see the “Supported Features” chapter.

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, you must enable Cisco express forwarding (CEF) switching on each NRP with the **ip cef** global configuration command.

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*.

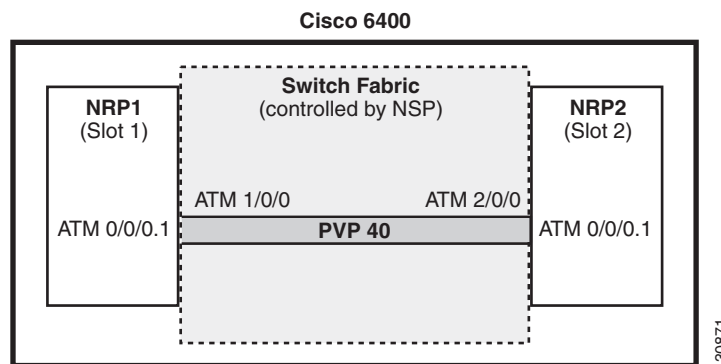
MPLS Edge LSRs Connected Through a PVP

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
```

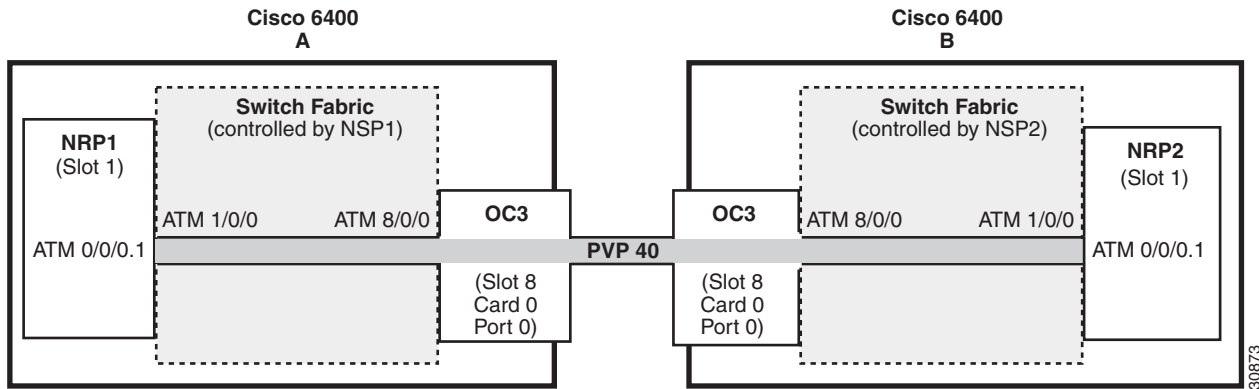
To complete the PVP connection between NRP1 and NRP2 in Figure 1, the NSP must be configured to set the path through the switch fabric. The following example shows the VP-switch configuration for the NSP:

```
NSP# configure terminal
NSP(config)# interface ATM1/0/0
NSP(config-if)# atm pvc 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
```

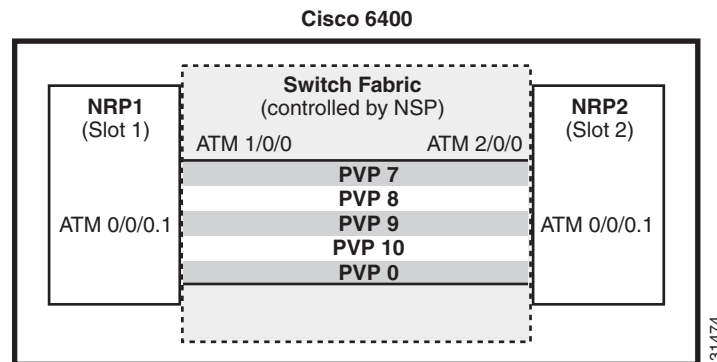
MPLS Edge LSRs Connected Through a VPI Range

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
```

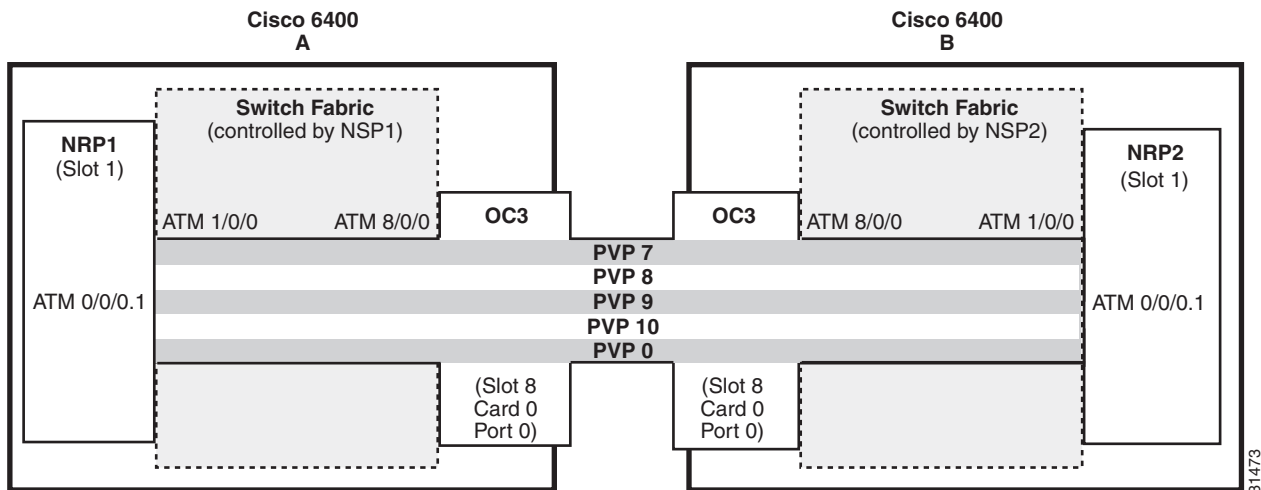
**Note**

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*.

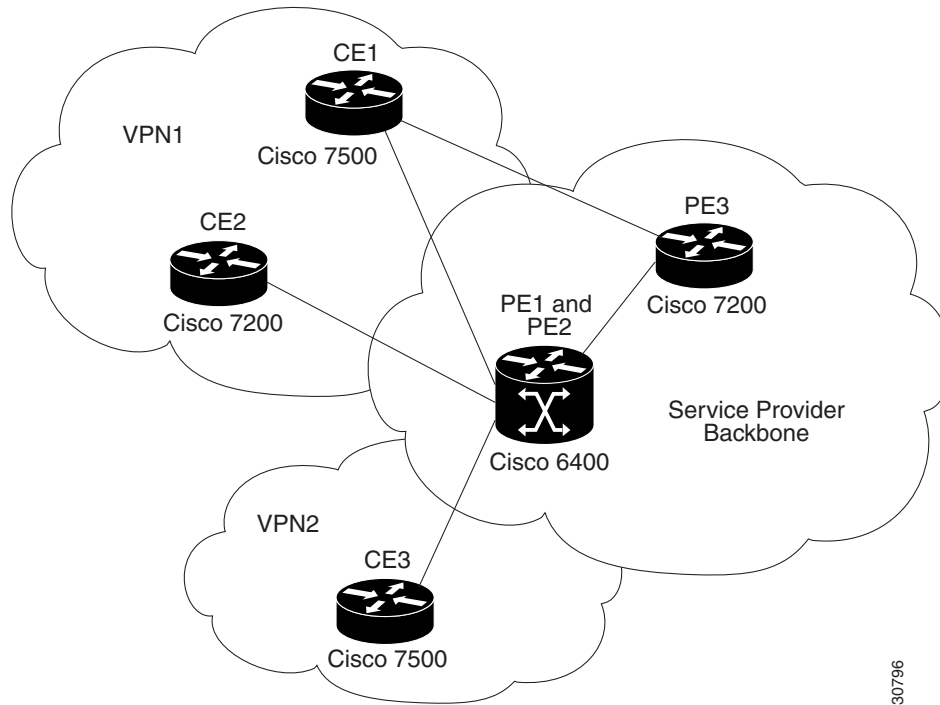
The examples in this section illustrate the configurations necessary to enable MPLS VPN on a Cisco 6400.

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



30796

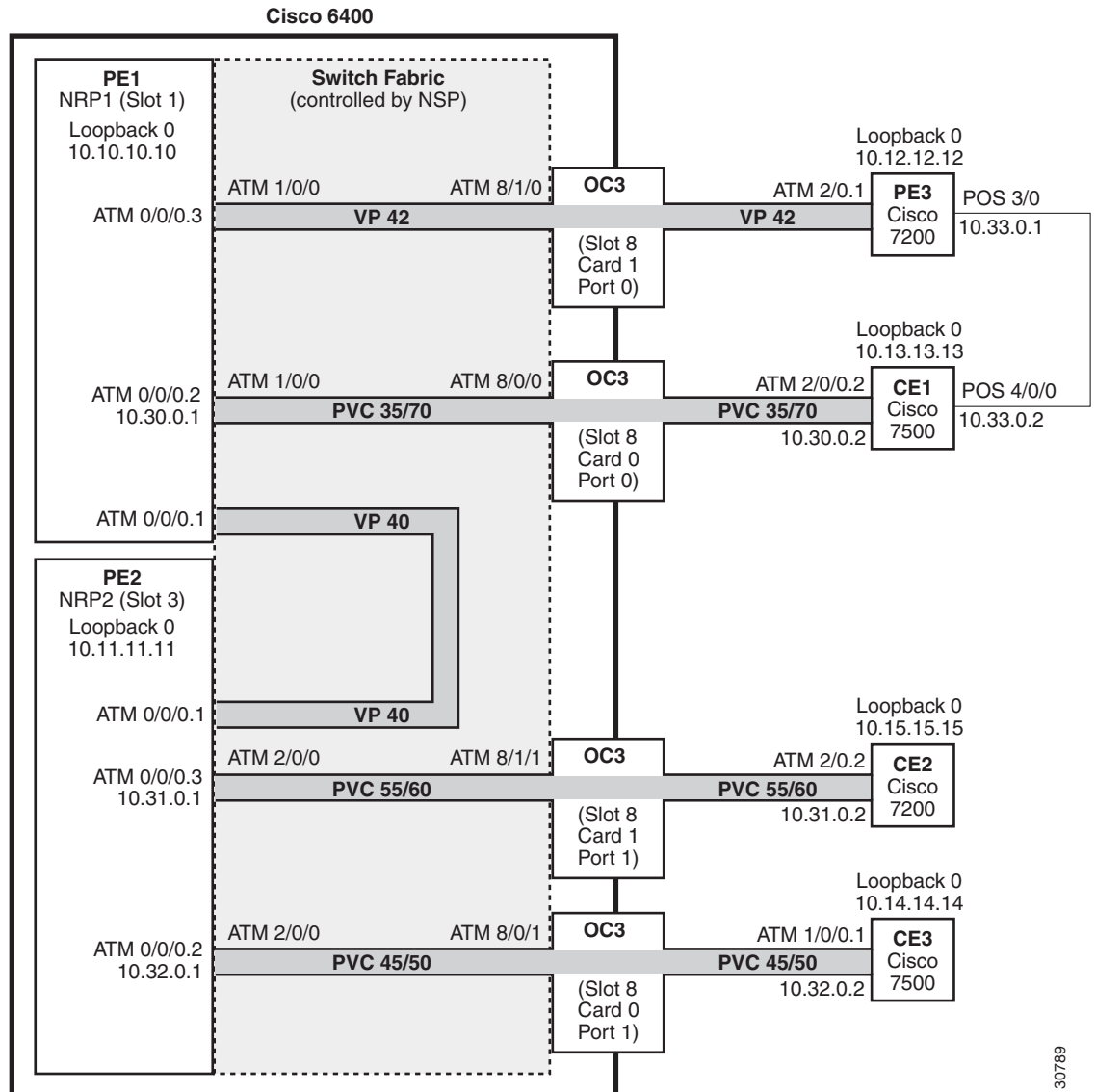
To enable a Cisco 6400 NRP to participate in a VPN, you must configure the NSP to create paths from the NRP through the Cisco 6400 switch fabric. The switch fabric provides the only connection between the NRP and an external port on a network line card (NLC). The switch fabric also provides the only 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



30789

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

```




Service Selection Gateway

This chapter describes the Service Selection Gateway (SSG) features supported in Cisco IOS Release 12.2(2)B and the RADIUS profiles, vendor-specific attributes and accounting records used with the SSG features. This chapter contains the following sections:

- Overview
- Restrictions
- Prerequisites
- Configuring Features
- RADIUS Accounting Records
- Configuring RADIUS Profiles
- Configuration Example
- Monitoring and Troubleshooting SSG

Overview

The SSG feature is a switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as xDSL, cable modems, or wireless to allow simultaneous access to network services.

The SSG with Web Selection works in conjunction with the Cisco Service Selection Dashboard (SSD) or its successor product, the Cisco Subscriber Edge Services Manager (SESM). Together with the SESM or SSD, SSG provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with an SESM or SSD web application using a standard Internet browser.

The SESM operates in two modes:

- RADIUS mode—This mode obtains subscriber and service information from a RADIUS server. SESM in RADIUS mode is similar to the SSD.
- DESS mode—The Directory-Enabled Service Selection (DESS) mode provides access to a Lightweight Directory Access Protocol (LDAP)-compliant directory for subscriber and service profile information. This mode also has enhanced functionality for SESM web applications and uses a role-based access control (RBAC) model to manage subscriber access.

This chapter provides information on general SSG configuration that applies to SESM in DESS mode and RADIUS mode. It also provides RADIUS-specific configuration information that only applies to SESM in RADIUS mode or SSD.

If your deployment uses SESM in DESS mode, these documents provide additional information on DESS-mode topics:

- For information on configuring SESM, see the *Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide*.
- For information on creating and maintaining subscriber, service, and policy information in an LDAP directory, see the *Cisco Distributed Administration Tool Guide*.

These documents can be found:

- On Cisco.com at:
Technical Documents: Aggregation: Cisco 6400 Carrier-Class Broadband Aggregator
- On the Documentation CD-ROM at:
Aggregation Solutions: Cisco 6400 Carrier-Class Broadband Aggregator

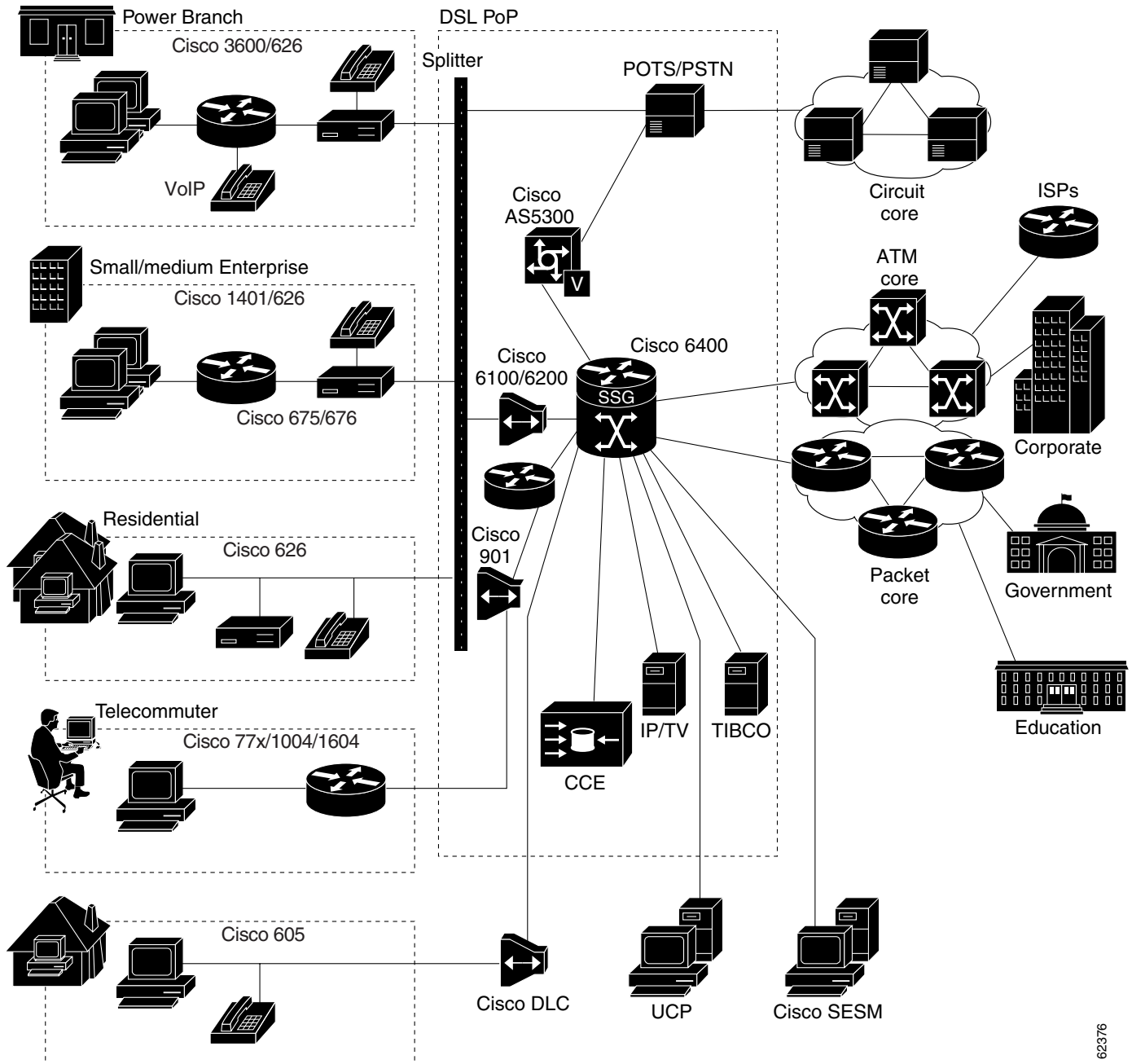
**Note**

The SESM and SSD functionality described in this document is available only with the SSG with Web Selection product.

In the rest of this chapter, all references to SESM also apply to SSD—unless a clear distinction is made.

Figure 4-1 shows a diagram of a sample network topology including the SSG. This is an end-to-end, service-oriented DSL deployment consisting of Digital Subscriber Line Access Multiplexers (DSLAMs), ADSL modems, and other internetworking components and servers. The SSG resides in the Cisco 6400 carrier-class broadband aggregator, which acts as a central control point for Layer 2 and Layer 3 services. This can include services available through Asynchronous Transfer Mode (ATM) virtual circuits (VCs), virtual private dial-up networks (VPDNs), or normal routing methods.

Figure 4-1 SSG Connection Between ADSL Equipment and Network Services



62376

The SSG communicates with the authentication, authorization, and accounting (AAA) management network where Remote Access Dial-In User Service (RADIUS), Dynamic Host Configuration Protocol (DHCP), and Simple Network Management Protocol (SNMP) servers reside and with the Internet service provider (ISP) network, which may connect to the Internet, corporate networks, and value-added services.

A licensed version of the SSG works with SESM to present to subscribers a menu of network services that can be selected from a single graphical user interface (GUI). This improves flexibility and convenience for subscribers, and enables service providers to bill subscribers based on connect time and services used, rather than charging a flat rate.

The user opens an HTML browser and accesses the URL of the SESM web server application. SESM forwards user login information to the SSG, which forwards the information to either the AAA server for the SSD or SESM in RADIUS mode, or to the RADIUS/DESS Proxy (RDP) component of SESM for SESM in DESS mode.

- If the user is not valid, the AAA server or RDP sends an Access-Reject message.
- If the user is valid, the AAA server or RDP sends an Access-Accept message with information specific to the user's profile about which services the user is authorized to use. The SSG logs the user in, creates a host object in memory, and sends the response to SESM.

Based on the contents of the Access-Accept response, SESM presents a menu of services that the user is authorized to use, and the user selects one or more of the services. The SSG then creates an appropriate connection for the user and optionally starts RADIUS accounting for the connection.

Note that when a non-Point-to-Point Protocol (non-PPP) user, such as in a bridged-networking environment, disconnects from a service without logging off, the connection remains open and the user can reaccess the service without going through the log in procedure. This is because no direct connection (PPP) exists between the subscribers and the SSG. To prevent non-PPP users from being logged in to services indefinitely, be sure to configure the Session-Timeout and/or Idle-Timeout RADIUS attributes.


Note

As of Cisco IOS Release 12.1(5)DC, a service object stays in the system after all users log off. The same service object is reused when a user logs on to the service again. The administrator can remove the service object by using the **clear ssg service** *service name* command if the administrator knows that the service is obsolete.

Benefits

Web-Based Interface

The SSG with Web Selection works with the Cisco SESM. The SESM is a specialized web server that allows users to log in to and disconnect from multiple passthrough and proxy services through a standard web browser.

After the user opens a web browser, the SSG allows access to a single IP address or subnet, referred to as the “default network.” This is typically the IP address of SESM. The SESM prompts the user for a username and password. After the user is authenticated, SESM presents a list of available services.

The SESM provides all the functionality of its predecessor product, the SSD. SESM also introduces the following functionality:

- Policy-based service subscription and self-care—Service providers can grant users certain privileges, including:
 - Subscribing to or unsubscribing from network services that the users are authorized to access
 - Creating subaccounts and subscribing services to them
 - Changing account details, such as passwords and billing address
- LDAP-compliant directory storage of service and subscriber information—LDAP provides:
 - Implementation of self-care by enabling dynamic user updates of subscriber and service information
 - Management of users as groups—Service providers can simply add services to user group profiles instead of individual user profiles

RADIUS Authentication and Accounting

The SSG is designed to work with RADIUS-based AAA servers that accept vendor-specific attributes (VSAs).

LDAP Directory

The SSG using SESM in DESS mode can use an LDAP directory as the data repository for service, subscriber, and policy information.

Multiple Traffic-Type Support

The SSG supports the following types of services:

- Passthrough Service

The SSG can forward traffic through any interface through normal routing or a next hop table. Because Network Address Translation (NAT) is not performed for this type of traffic, overhead is reduced. Passthrough service is ideal for standard Internet access.

- Proxy Service

When a subscriber requests access to a proxy service, the SSG proxies the Access-Request to the remote AAA server. Upon receiving an Access-Accept from the remote RADIUS server, the SSG logs in the subscriber. To the remote AAA server, the SSG appears as a client.

During remote authentication, if the RADIUS server assigns an IP address to the subscriber, the SSG performs NAT between the assigned IP address and the subscriber's real IP address. If the remote RADIUS server does not assign an IP address, NAT is not performed.

When a user selects a proxy service, there is another username and password prompt. After authentication, the service is accessible until the user logs out from the service, logs out from SESM, or is timed out.

- Transparent Passthrough—Supported only in Cisco IOS Releases 12.0(3)DC and 12.0(5)DC

When enabled, transparent passthrough allows unauthenticated subscriber traffic to be routed through the SSG in either direction. Filters can be specified to control transparent passthrough traffic. Some of the applications for this feature include:

- Making the SSG easy to integrate into an existing network by not requiring users who have authenticated with network access servers (NAS) to authenticate with the SSG
- To allow management traffic (such as TACACS+, RADIUS, and SNMP) from NASes connected to the host network to pass through to the service provider network
- To allow visitors or guests to access certain parts of the network

- Multicast

The SSG supports multicast traffic, which includes normal multicast packets and Internet Group Management Protocol (IGMP) packets.

In order for the SSG to forward multicast packets to the IOS routing engine, it must be configured as follows:

- The interface where multicast packets are received must be configured as an uplink or downlink interface, or a service must be bound to the interface. An uplink interface is an interface to services; a downlink interface is an interface to subscribers.
- SSG multicast must be enabled, in addition to IOS multicast.

If multicast is not enabled, multicast packets received on the interface are dropped.

- PPP Termination Aggregation (PTA) and PTA Multi-Domain (PTA-MD)

PPP Termination Aggregation (PTA) can only be used by PPP-type users. AAA is performed exactly as in the proxy service type. A subscriber logs in to a service by using a PPP dialer application with a username of the form `user@service`. The SSG recognizes the `@service` as a service profile and loads the service profile from the local configuration or a AAA server. The SSG forwards the AAA request to the remote RADIUS server as specified by the service profile's RADIUS-Server Attribute. An address is assigned to the subscriber through RADIUS Attribute 8 or Cisco-AVpair "ip:addr-pool." NAT is not performed, and all user traffic is aggregated to the remote network. With PTA, users can only access one service. Users do not have access to the default network or the SESM.

While PTA terminates the PPP session into a single routing domain, PTA-MD terminates the PPP sessions into multiple IP routing domains, thus supporting a wholesale VPN model where each domain is isolated from the other by an ATM core and has the capability to support overlapping IP addresses.

Packet Filtering

The SSG uses IOS access control lists (ACLs) to prevent users, services, and passthrough traffic from accessing specific IP addresses and ports.

- Services

When an ACL attribute is added to a service profile, all users of that service are prevented from accessing the specified IP address, subnet mask, and port combinations through the service.

- Users

When an ACL attribute is added to a user profile, it applies globally to all the user's traffic.

- Transparent Passthrough—Supported only in Cisco IOS Releases 12.0(3)DC and 12.0(5)DC

Upstream and downstream attributes, including `inacl` and `outacl` attributes, can be added to a special pseudo-service profile that can be downloaded to the SSG from a RADIUS server. Additionally, locally configured ACLs can be used. After the ACLs have been defined, they are applied to all traffic passed by the transparent passthrough feature.

Service Access Order

When users are accessing multiple services, the SSG must determine the services for which the packets are destined. To do this, the SSG uses an algorithm to create a service access order list that is stored in the user's host object and contains services that are currently open and the order in which they are searched.

The algorithm that creates this list orders the open services based on the size of the network, which is determined by the subnet mask of the Service Route RADIUS attribute. A subnet that contains more hosts implies a larger network. In the case of networks that are the same size, the services are listed in the order in which they were last accessed.

When creating service profiles, be sure to define as small a network as possible. If there is overlapping address space, packets might be forwarded to the wrong service.

Next Hop Gateway

The next hop gateway attribute is used to specify the next hop key for a service. Each SSG uses its own next hop gateway table that associates this key with an actual IP address.

Note that this attribute overrides the IP routing table for packets destined to a service.

DNS Redirection

When the SSG receives a DNS request, it performs domain name matching by using the Domain Name attribute from the service profiles of the currently logged in services.

If a match is found, the request is redirected to the DNS server for the matched service.

If a match is not found and the user is logged in to a service that has Internet connectivity, the request is redirected to the first service in the user's service access order list that has Internet connectivity. Internet connectivity is defined as a service containing a Service Route attribute of 0.0.0.0/0.

If a match is not found and the user is not logged in to a service that has Internet connectivity, the request is forwarded to the DNS server defined in the client's Transmission Control Protocol/Internet Protocol (TCP/IP) stack.

Fault Tolerance for DNS

The SSG can be configured to work with a single DNS server, or two servers in a fault-tolerant configuration. Based on an internal algorithm, DNS requests are switched to the secondary server if the primary server fails to respond with a DNS reply within a certain time limit.

Session-Timeout and Idle-Timeout RADIUS Attributes

In a dial-up networking or bridged (non-PPP) network environment, a user can disconnect from the NAS and release the IP address without logging out from the SSG. If this happens, the SSG continues to allow traffic to pass from that IP address, and this can be a problem if the IP address is obtained by another user.

The SSG provides two mechanisms to prevent this problem:

- Idle-Timeout attribute—Specifies the maximum time a session or connection can remain idle before it is disconnected.
- Session-Timeout attribute—Specifies the maximum amount of time a host or service object can remain active at any one time.

The Session-Timeout and Idle-Timeout attributes can be used in either a user or service profile. In a user profile, the attribute applies to the user's session. In a service profile, the attribute individually applies to each service connection.

Concurrent or Sequential Service Access Mode

SSG services can be configured for concurrent or sequential access. Concurrent access allows users to log in to this service while simultaneously connected to other services. Sequential access requires that the user log out of all other services before accessing a service configured for sequential access.

Concurrent access is recommended for most services. Sequential access is ideal for services for which security is important, such as corporate intranet access, or for which there is a possibility of overlapping address space.

Extended High System Availability

The SSG supports extended high system availability (EHSA) redundancy. You can configure this chassis redundancy at the slot level of the Cisco 6400 for adjacent slot or subslot pairs. For example, if you have SSGs installed in slots 1 and 2, you can set a preferred device between the two. To ensure that configuration is consistent between redundant SSGs, you can configure automatic synchronization between the two SSGs. You can also manually force the primary and secondary devices in a redundant pair to switch roles. See the *Cisco 6400 Software Setup Guide* for more information on EHSA redundancy.

Web Selection of L2TP Service Type

SSG supports L2TP. When a subscriber selects a service through SESM, the NRP as an L2TP access concentrator (LAC) sends the PPP session through the service specific L2TP tunnel. If the tunnel does not already exist, the NRP-LAC creates the proper tunnel to the L2TP network server (LNS).

Local Forwarding

SSG can be enabled to forward packets locally between directly connected subscribers.

SSG Single Host Logon

To log in to a service through SESM, a subscriber has to log in only twice: once for the PPP session and once for the service.

SSG Host Key



Note

All references to SESM also apply to SSD unless a clear distinction is made.

The SSG Host Key feature enhances communication and functionality between SSG and SESM.

With the SSG Host Key feature, SSG performs port address translation (PAT) and NAT on the HTTP traffic between the subscriber and the SESM server. When a subscriber sends an HTTP packet to the SESM server, SSG creates a port map that changes the source IP address to a configured SSG source IP address and changes the source TCP port to a port allocated by SSG. The SSG assigns a bundle of ports to each subscriber because one subscriber can have several simultaneous TCP sessions when accessing a web page. The assigned *host key*, or combination of port bundle and SSG source IP address, uniquely identifies each subscriber. The host key is carried in RADIUS packets sent between the SESM server and SSG as a Host-Key vendor-specific attribute. When the SESM server sends a reply to the subscriber, SSG translates the destination IP address and destination TCP port according to the port map.

For each TCP session between a subscriber and the SESM server, SSG uses one port from the port bundle as the port map. Port mappings are flagged as eligible for reuse based on inactivity timers, but are not explicitly removed once assigned. The number of port bundles are limited, but you can assign multiple SSG source IP addresses to accommodate more subscribers.

SSG assigns the base port of the port bundle to a port map only if SSG has no state information for the subscriber, or if the state of the subscriber has changed. When the SESM server sees the base port of a port bundle in the host key, SESM knows that it needs to query SSG for new subscriber state information.

The SSG Host Key feature provides the following benefits:

- Support for Overlapped Subscriber IP Addresses Extended to Include SESM Usage
- Cisco SESM Provisioning for Subscriber and SSG IP Addresses Is No Longer Required
- Reliable and Just-in-Time Notification to Cisco SSD of Subscriber State Changes
- Support for Additional Data in Subscriber Account Queries
- Support for Multiple Accounts for One Subscriber IP Address

Support for Overlapped Subscriber IP Addresses Extended to Include SESM Usage

Without the SSG Host Key feature, PPP users are allowed to have overlapped subscriber IP addresses, but they cannot use SSG with Web Selection to conduct service selection through the web-based SESM user interface.

With the SSG Host Key feature, PPP users can have overlapped IP addresses while using SSG with Web Selection. The subscriber IP addresses are also not required to be routable within the service management network where the SESM server resides, because the host key enables support for private addressing schemes.

Cisco SESM Provisioning for Subscriber and SSG IP Addresses Is No Longer Required

Without the SSG Host Key feature, SESM must be provisioned for subscriber and SSG IP addresses before SESM is able to send RADIUS packets to SSG, or send HTTP packets to subscribers.

The SSG Host Key feature eliminates the need to provision SESM in order to allow one SESM server to serve multiple SSGs, and to allow one SSG to be served by multiple SESM servers.

Reliable and Just-in-Time Notification to Cisco SSD of Subscriber State Changes

Without the SSG Host Key feature, SSG uses an asynchronous messaging mechanism to immediately notify the SESM server of subscriber state changes in SSG (such as session time outs or idle time-out events).

The SSG Host Key feature replaces the asynchronous messaging mechanism with an implicit and reliable notification mechanism that uses the base port of a port bundle to alert the SESM server of a state change. The SESM server can then query SSG for the true state of the subscriber and update the cached object or send the information back to the subscriber.

Support for Additional Data in Subscriber Account Queries

The SESM server queries SSG and receives the following information in reply:

- Account Query—If a subscriber logs in his account, SSG replies with subscriber state information, including a list of services to which the subscriber has logged on.
- Service Query—If a subscriber logs in to a particular service, SSG replies with information on the subscriber's usage of the service.
- Profile Query—SSG replies with the full profile of a PPP user.

The subscriber can query its account status manually or automatically. Each account query results in an update of the SESM user interface. The SSG Host Key feature enables the account query reply to include additional information, such as an account token.

Support for Multiple Accounts for One Subscriber IP Address

To accommodate multiple users sharing a single PC, the SSG Host Key feature supports multiple subaccounts each with a different username under one subscriber. When the SESM server contacts SSG to log in a new user to an already logged in account, SSG logs off the existing account and logs in the new user. In account switching, the port bundle and host object remain the same, but the content of the host object is changed according to the profile of the subaccount user.

Restrictions

Open Garden

Do not bind an open garden service to an interface that is bound to another service. Use the **show ssg binding** privileged EXEC command to view services and the interfaces to which they have been bound.

CEF

CEF works with Point-to-Point Protocol over Ethernet (PPPoE) only and does not work with Fast Ethernet.

SSG does not support simultaneous use of Cisco Express Forwarding (CEF) and Routed Bridge Encapsulation (RBE).

VPI/VCI Indexing to Service Profile

VPI/VCI indexing to service profile only works for Point-to-Point Protocol over ATM (PPPoA).

Proxy RADIUS Enhancements

For the proxy RADIUS enhancements, the sizes of the user-defined *string* and full username are limited to the smaller of the following values:

- 246 bytes (10 bytes less than the standard RADIUS protocol limitation)
- *Max* - 10 bytes, where *Max* is the maximum size of the RADIUS attribute supported by your proxy RADIUS server

TCP Redirect - Logon

If you use SSD as a captive portal, this feature requires Cisco SSD Release 3.0(1). Alternately, you can use any release of Cisco SESM.

Host Key

- All SSG source IP addresses configured with the **ssg port-map source ip** command must be routable in the management network where the SESM resides.
- For each SESM server, all connected SSGs must have the same port-bundle length.
- RFC1483 or local bridged/routed clients cannot have overlapped IP addresses, even across different interfaces.
- Enabling the Host Key feature requires an SSG reload and an SESM restart to take effect.
- The Host Key feature must be separately enabled at the SESM and at all connected SSGs or not at all.

Prerequisites

Cisco Subscriber Edge Services Manager

If you want to perform Layer 3 service selection, you must install and configure the Cisco SESM as described in the *Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide*.

Single Host Logon

In order to use the Single Host Logon feature, you must install and configure Cisco SESM or Cisco SSD version 2.5 or later versions.

Layer 2 Tunnel Protocol

To achieve 2000 L2TP sessions, you need at least 128 MB of DRAM on the NRP.

Host Key

The SSG Host Key feature requires Cisco SSD Release 3.0(1) or Cisco SESM Release 3.1(1). If you are using an earlier release of SSD, disable the SSG Host Key feature with the **no ssg port-map enable** global configuration command.

Configuring Features

This section contains the following tasks that apply to the SSG when used with SSD or with SESM in RADIUS or DESS mode:

- Enabling SSG
- Configuring Local Service Profiles
- Configuring Security
- Configuring a Default Network
- Configuring Interfaces
- Configuring Services
- Configuring Fastswitching
- Configuring Multicast
- Configuring RADIUS Interim Accounting
- Configuring Cisco Express Forwarding
- Configuring IOS Network Address Translation
- Configuring VPI/VCI Indexing to Service Profile
- Configuring SSG with L2TP Service Type
- Configuring Local Forwarding
- Configuring an Open Garden
- Configuring TCP Redirect - Logon
- Configuring Host Key

**Note**

The following tasks apply to the SSG only when used with SSD or with SESM in RADIUS mode:

- Configuring AAA Server Group Support for Proxy Services
- Configuring the Proxy RADIUS Enhancements

Enabling SSG

As of Cisco IOS Release 12.0(7) DC, SSG is disabled by default. To enable SSG, enter the following command in global configuration mode:

Command	Purpose
Router(config)# ssg enable	Enables SSG functionality.

Verifying that SSG Is Enabled

To verify that SSG is enabled, enter the EXEC command **show running-config**.

Configuring Local Service Profiles

This task is required if you want to use Layer 2 service selection; otherwise, it is optional. You can configure local service profiles in addition to the service profiles on the remote RADIUS server. See the “Configuring RADIUS Profiles” section on page 4-39 for information on configuring service profiles on the remote RADIUS server.

Command	Purpose
Router(config)# local-profile <i>profilename</i>	Enters profile configuration mode. Configures a local RADIUS service profile.
Router(config-prof)# attr <i>radius-attribute-id</i> [<i>vendor-id</i>] [<i>cisco-vs-a-type</i>] <i>attribute-value</i>	Configures an attribute in a local RADIUS service profile.

Verifying Local Service Profiles

Enter the **show running-config** command to verify that local service profiles have been configured correctly.

Configuring Security

Command	Purpose
Router(config)# aaa new-model	Enables AAA.
Router(config)# aaa authentication ppp default radius	Specifies RADIUS as the default authentication method for users that log in to serial interfaces by using PPP.
Router(config)# aaa authorization network default radius	Specifies that RADIUS is the default authorization used for all network-related requests.
Router(config)# radius-server host {hostname ip-address} [auth-port UDP-port-number] [acct-port UDP-port-number]	Specifies the RADIUS server host.
Router(config)# radius-server key AAAPassword	Sets the RADIUS shared secret between the SSG and the local AAA server.
Router(config)# radius-server vsa send	(Optional) Send vendor-specific attributes with authentication and accounting requests to the AAA server.
Router(config)# ssg radius-helper key DashboardPassword	Sets the RADIUS shared secret between SSG and SESM.
Router(config)# ssg radius-helper [auth-port UDP-port-number] [acct-port UDP-port-number]	Specifies the UDP default port numbers for a RADIUS authentication server (1645) and accounting server (1646).
Router(config)# ssg service-password ServicePassword	Sets the password used to authenticate the SSG with the local AAA server service profiles. This value must match the value configured for the AAA server service profiles.

Verifying Security

Enter the **show running-config** command to verify that security has been configured correctly.

Configuring a Default Network

Configure the first IP address or subnet that users are able to access without authentication. This is the address where the Cisco SESM resides.

Command	Purpose
Router(config)# ssg default-network ip-address mask	Sets the IP address or subnet that users are able to access without authentication. Typically, this is the address where the Cisco SESM resides. A mask provided with the IP address specifies the range of IP addresses that users are able to access without authentication.

Verifying the Default Network

Enter the **show running-config** command to verify that the default network has been configured correctly.

Configuring Interfaces

If you are going to use PPP to connect subscribers to the SSG, you do not have to configure any downlink interfaces. If you are using non-PPP connections, such as bridging or LAN, you must configure at least one downlink interface.

Command	Purpose
<pre>Router(config)# ssg bind direction downlink {ATM atm-interface Async async-interface BVI bvi-interface Dialer dialer-interface Ethernet ethernet-interface FastEthernet fastethernet-interface Group-Async group-async-interface Lex lex-interface Loopback loopback-interface Multilink multilink-interface Null null-interface Port-channel port-channel-interface Tunnel tunnel-interface Virtual-Access virtual-access-interface Virtual-Template virtual-template-interface Virtual-TokenRing virtual-tokenring-interface}</pre>	Specifies a downlink interface, that is, the interface to the subscribers.

Configure all interfaces that are connected to services as uplink interfaces.

Command	Purpose
<pre>Router(config)# ssg bind direction uplink {ATM atm-interface Async async-interface BVI bvi-interface Dialer dialer-interface Ethernet ethernet-interface FastEthernet fastethernet-interface Group-Async group-async-interface Lex lex-interface Loopback loopback-interface Multilink multilink-interface Null null-interface Port-channel port-channel-interface Tunnel tunnel-interface Virtual-Access virtual-access-interface Virtual-Template virtual-template-interface Virtual-TokenRing virtual-tokenring-interface}</pre>	Specifies an uplink interface, that is, the interface to the services.

Verifying Interfaces

Enter the **show ssg direction** command to verify that interfaces have been configured correctly.

Configuring Services



Note Every service must be bound to an uplink interface.

Command	Purpose
<pre>Router(config)# ssg bind service service {ip-address ATM atm-interface Async async-interface BVI bvi-interface Dialer dialer-interface Ethernet ethernet-interface FastEthernet fastethernet-interface Group-Async group-async-interface Lex lex-interface Loopback loopback-interface Multilink multilink-interface Null null-interface Port-channel port-channel-interface Tunnel tunnel-interface Virtual-Access virtual-access-interface Virtual-Template virtual-template-interface Virtual-TokenRing virtual-tokenring-interface}</pre>	Specifies the interface for a service.
<pre>Router(config)# ssg service-search-order local remote local remote remote local</pre>	(Optional) Specifies the order in which SSG searches for a service profile. The default service search order is local remote, that is, the SSG searches for service profiles in Flash memory first, then on the RADIUS server.
<pre>Router(config)# ssg next-hop download [profile-name] [profile-password]</pre>	(Optional) Downloads the next-hop table from a RADIUS server.
<pre>Router(config)# ssg maxservice number</pre>	(Optional) Sets the maximum number of services per user. The default is 10.

Verifying Services

Enter the **show ssg service** command to verify that services have been bound to interfaces correctly. Enter the **show running-config** command to verify that the service search order and maximum services have been configured correctly. Enter the **show ssg next-hop** command to verify all mappings between services and IP addresses.

Configuring Fastswitching



Note This task is optional. Fastswitching is enabled by default.

Command	Purpose
<pre>Router(config)# ssg fastswitch</pre>	Enables fastswitching.
<pre>Router(config)# no ssg fastswitch</pre>	Disables fastswitching.

Verifying Fastswitching

Enter the **show running-config** command to verify that fastswitching has been enabled. Because fastswitching is enabled by default, it is not displayed in the running configuration. If fastswitching has been disabled, the following line appears in the output of the **show running-config** command:

```
no ssg fastswitch
```

Configuring Multicast



Note

This task is optional. Multicast is disabled by default.

Command	Purpose
Router(config)# ssg multicast	Enables multicast. When multicast is enabled, the SSG forwards multicast packets, which include normal multicast packets and IGMP packets, received on an uplink or downlink interface that has had a service bound to it to the IOS routing engine.
Router(config)# no ssg multicast	Disables multicast. If multicast is disabled, multicast packets received on an uplink or downlink interface or an interface that has had a service bound to it will be dropped.

Verifying Multicast

Enter the **show running-config** command to verify that multicast has been enabled. If multicast is disabled, which is the default, it will not be displayed in the running configuration. If multicast is enabled, the following line will appear in the output of the **show running-config** command:

```
ssg multicast
```

Configuring RADIUS Interim Accounting

The SSG supports intermittent RADIUS accounting updates. When a user logs in to the SSG, the SSG sends an accounting start record to the local RADIUS server. When a user logs in to a service, the SSG sends a connection start record to the local RADIUS server and to the remote RADIUS proxy server. During the time that the user is logged in to the SSG, the SSG sends accounting update records at specified intervals to the appropriate server. When a user logs off from a service, the SSG sends a connection stop record to the local RADIUS server and to the remote RADIUS proxy server. When a user logs off from the SSG, the SSG sends an accounting stop record to the local RADIUS server. See “Configuration Example” for more information.

This task is optional. Set the interval at which accounting updates are sent to the accounting server.

Command	Purpose
Router(config-if)# ssg accounting interval <i>seconds</i>	Specifies the interval at which accounting updates are sent to the accounting server. The minimum interval is 60 seconds. The default interval is 120 seconds.

Verifying Interim Accounting

Enter the **show running-config** command to verify that the accounting interval has been set correctly.

Configuring Cisco Express Forwarding



Note

CEF works with Point-to-Point Protocol over Ethernet (PPPoE) only and does not work with Fast Ethernet.

SSG does not support simultaneous use of Cisco Express Forwarding (CEF) and Routed Bridge Encapsulation (RBE).

The SSG works with Cisco Express Forwarding (CEF) switching technology to provide maximum Layer 3 switching performance. Because CEF is topology-driven rather than traffic-driven, its performance is unaffected by network size or dynamics.



Note

This task is optional. CEF is disabled by default. CEF only works with PPPoE.

Command	Purpose
Router(config)# ip cef	Enables global IP CEF.

Verifying Cisco Express Forwarding

Enter the **show running-config** and **show ip cef** commands to verify that CEF has been enabled.

Configuring IOS Network Address Translation

The SSG uses IOS Network Address Translation (NAT) to map the inside IP addresses of subscribers to the outside IP addresses from the destination service networks. This replaces the SSG NAT used in Cisco IOS Release 12.0(3)DC.

To configure IOS Network Address Translation (NAT), you must specify an inside interface from which clients connect to the SSG and an outside interface from which services are accessed. Enter interface or subinterface configuration mode for the desired inside and outside interfaces and enter the appropriate command below.

**Note**

This task is optional.

Command	Purpose
Router(config-if)# ip nat inside	Specifies the inside interface from which clients access the SSG.
Router(config-subif)# ip nat outside	Specifies the outside interface from which services are accessed.

Verifying IOS Network Address Translation

Enter the **show running-config** command to verify that inside and outside ports have been specified correctly. Enter the **show ip nat translations** command to view your NAT addresses.

Configuring VPI/VCI Indexing to Service Profile

**Note**

VPI/VCI indexing to service profile only works for Point-to-Point Protocol over ATM (PPPoA).

The SSG supports virtual path identifier/virtual channel identifier (VPI/VCI) closed user groups by allowing VPI/VCIs to be bound to a given service. All users accessing the SSG through the VPI/VCI or range of VPI/VCIs will be able to access the service. You can specify whether users are allowed to access only the bound service or other additional services to which they subscribe. A closed user group service can only be selected through the VPI/VCI and not by entering the domain name in the user name of a Point-to-Point Protocol (PPP) session.

To configure VPI/VCI closed user groups, you must bind VPI/VCIs to a given service as described below. Closed user groups allow all users accessing the SSG through the VPI/VCI or range of VPI/VCIs to access the service. You can specify whether users are allowed to access only the bound service or other additional services to which they subscribe. A closed user group service can only be selected through the VPI/VCI and not by entering the domain name in the user name of a PPP session.

**Note**

This task is optional.

Command	Purpose
Router(config)# ssg vc-service-map <i>service-name</i> [interface <i>slot-module-port</i>] start-vpi start-vpi/vci [end-vpi end-vpi/vci] exclusive non-exclusive	Map VCs to service names.

Verifying VPI/VCI Indexing to Service Profile

Enter the **show running-config** and **show ssg vc-service-map** command to view service name to VC mappings.

Monitoring VPI/VCI Indexing to Service Profile

Command	Purpose
Router# show ssg vc-service-map	Displays VC to service name mappings.

Configuring SSG with L2TP Service Type



Note

Before configuring this feature, see the prerequisites for Layer 2 Tunnel Protocol.

To configure SSG with L2TP Service Type, perform the following tasks:

- Configuring the NRP as a LAC
- Configuring the RADIUS Profiles for SSG Support of L2TP
- Configuring the LNS

Configuring the NRP as a LAC

To configure the Cisco 6400 NRP as a LAC, enter the following command in global configuration mode:

Command	Purpose
Router(config)# vpdn enable	Enables L2TP functionality.

Verifying the NRP-LAC Configuration

To verify the NRP-LAC configuration, enter the EXEC command **show running-config**.

Configuring the RADIUS Profiles for SSG Support of L2TP

The following vendor-specific attributes are used by the SSG to support L2TP:

- Cisco-AVpair VPDN Attributes
- Account-Info VPDN Attribute
- Service-Info VPDN Attribute

For general information on configuring RADIUS profiles for SSG, see the “Configuring RADIUS Profiles” section.

Cisco-AVpair VPDN Attributes

Table 4-1 lists the Cisco-AVpair attributes used in the service profile to configure VPDN.

Table 4-1 Cisco AVPair Attributes

Attribute	Usage
VPDN IP Address	Specifies the IP addresses of the home gateways (LNSes) to receive the L2TP connections.
VPDN Tunnel ID	Specifies the name of the tunnel that must match the tunnel ID specified in the LNS VPDN group.
L2TP Tunnel Password	Specifies the secret (password) used for L2TP tunnel authentication.

Account-Info VPDN Attribute

Table 4-2 lists the Account-Info attribute used in the user profile to subscribe the user to a VPDN service.

Table 4-2 Account-Info Attribute

Attribute	Usage
Auto Service	Subscribes the user to a service. There can be multiple instances of this attribute within a single user profile. Use one attribute for each service to which the user is subscribed (reply attribute).

Service-Info VPDN Attribute

Table 4-3 lists the Service-Info attribute used in the service profile to define the L2TP service parameter.

Table 4-3 Service-Info Attributes

Attribute	Usage
Type of Service	Indicates whether the service is proxy (requiring remote authentication) or passthrough (does not require authentication). The default is passthrough.
MTU Size	Specifies the PPP MTU size of the SSG as an L2TP access concentrator (LAC). By default, the PPP MTU size is 1500 bytes. Note SESM in DESS mode does not support use of this attribute.

Verifying the RADIUS Profile Configurations

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

Configuring the LNS

To configure the LNS, typically a Cisco 7200 or another NRP, enter the following commands beginning in global configuration mode.

	Command	Purpose
Step 1	Router(config)# username <i>name</i> password <i>secret</i>	Specifies the password to be used for PAP and CHAP. Each subscriber requires a unique username and password.
Step 2	Router(config)# vpdn-group <i>number</i>	Selects the VPDN group. Each L2TP tunnel requires a unique VPDN group.
Step 3	Router(config-vpdn)# accept-dialin <i>l2tp</i> virtual-template <i>number</i>	Accepts incoming L2TP tunnel connections. Also specifies the virtual template interface to use to clone the new virtual access interface.
Step 4	Router(config-vpdn)# terminate-from <i>hostname</i> <i>hostname</i>	Specifies the tunnel ID that will be required when accepting a VPDN tunnel. This must match the VPDN tunnel ID configured in the RADIUS service profile.
Step 5	Router(config-vpdn)# l2tp tunnel password <i>password</i>	Identifies the password that the router will use for tunnel authentication.
Step 6	Router(config-vpdn)# exit	Returns to global configuration mode.
Step 7	Router(config)# interface Virtual-Template <i>number</i>	Creates a virtual template interface that can clone new virtual access interfaces.
Step 8	Router(config-if)# ip unnumbered <i>interface-type</i> <i>interface-number</i>	Configures the interface as unnumbered and provides a local address.
Step 9	Router(config-if)# peer default ip address <i>pool</i> <i>pool-name</i>	Specifies the pool from which to retrieve the IP address to assign to a remote peer dialing in to the interface.
Step 10	Router(config-if)# ppp authentication { chap chap pap pap chap pap }	Specifies the order in which the CHAP or PAP protocols are requested on the interface.

L2TP Examples

This section provides the following configuration examples:

- SSG as a LAC Example
- RADIUS User Profile Example
- RADIUS Service Profile Example
- LNS Configuration Example

SSG as a LAC Example

The following example shows a basic SSG configuration for a LAC:

```
!
vpdn enable
ssg enable
!
```

RADIUS User Profile Example

The following example shows a basic RADIUS user profile for SSG support of L2TP:

```
user = l2tp_user{
member = Some-Users
radius=CSUNIX_RADIUS_DICTIONARY_for_6400-NRP-SSG-v1.0 {
check_items= {
2=cisco
}
reply_attributes= {
6=2
7=1
9,250="Nl2tp_tunnel.com"
}
}
}
```

RADIUS Service Profile Example

The following example shows a basic RADIUS service profile for SSG support of L2TP:

```
reply_attributes= {
9,251="R10.6.6.0;255.255.255.0"
9,251="ODomain.com"
9,251="D10.7.7.7;10.7.7.8"
9,251="ITunnel1"
9,251="TT"
9,251="B1500"
9,251="S10.7.7.7;1645;1646;cisco"
9,1="vpdn:ip-addresses=10.8.8.8"
9,1="vpdn:tunnel-id=My-Tunnel"
9,1="vpdn:l2tp-tunnel-password=cisco"
```

LNS Configuration Example

The following example shows a basic LNS configuration:

```
!
username l2tp_user password 0 cisco
vpdn-group 1
  accept-dialin
  protocol l2tp
  virtual-template 1
  terminate-from hostname My-Tunnel
  l2tp tunnel password 7 02050D480809
!
interface Virtual-Template1
  ip unnumbered FastEthernet0/0
  no ip directed-broadcast
  peer default ip address pool pool2
  ppp authentication pap chap
!
```

Monitoring L2TP

The following privileged EXEC commands will help you monitor and maintain the SSG support of L2TP.

Command	Purpose
<code>show ssg l2x {dialer-config dialer-list dialer-status info vpdn-group} service-name</code>	Displays SSG L2TP information, including dialer configuration, dialer-list tables, tunnel information, and vpdn-group information.
<code>show vpdn tunnel [all packets state summary transport] [id local-name remote-name]</code>	Displays VPDN tunnel information including tunnel protocol, ID, packets sent and received, receive window sizes, retransmission times, and transport status.
<code>show vpdn session [all [interface tunnel username] packets sequence state timers window]</code>	Displays VPDN session information including interface, tunnel, username, packets, status, and window statistics.
<code>clear vpdn tunnel l2tp remote-name local-name</code>	Shuts down a specific tunnel and all the sessions within the tunnel.

Configuring Local Forwarding

To enable SSG to forward packets locally, enter the following command in global configuration mode:

Command	Purpose
<code>Router(config)# ssg local-forwarding</code>	Enables local forwarding.

Example: Local Forwarding

In the following configuration, local forwarding is enabled:

```
!
 ssg enable
→ ssg local-forwarding
!
```

Verifying Local Forwarding

To verify that you enabled local forwarding, enter the **show running-config** EXEC command.

Configuring an Open Garden



Note Before configuring this feature, see the restrictions for Open Garden.

An “open garden” is a collection of websites or networks that users can access as long as they have physical access to the network. Users do not need to provide authentication information before accessing the websites in the open garden. A “walled garden,” on the other hand, refers to a collection of websites or networks that users can access after providing minimal authentication information.

SSG handles the default network and the open garden as services that have associated domain names and DNS addresses. As many as 100 domains can be associated with the open garden. If a subscriber creates a DNS request for one of those domain names, the DNS request is resolved by the SSG to the default network. This ensures that a subscriber can access SESM, which typically resides on the management network with a private address, even when the subscriber is assigned a public DNS server.



Note RADIUS accounting records are not created for open garden services.

To configure an open garden, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# local-profile <i>profile-name</i>	Creates a local service profile and enters profile configuration mode.
Step 2	Router(config-prof)# attribute 26 9 251 <i>"Rip-address;subnet-mask"</i> (Repeat step as necessary.)	(Service Route attribute) Specifies the network available to the service. You can add multiple networks to an open garden service.
Step 3	Router(config-prof)# attribute 26 9 251 <i>"Dip-address"</i>	(DNS Server Address attribute) Specifies the DNS server for the service.
Step 4	Router(config-prof)# attribute 26 9 251 <i>"Odomain-name"</i> (Repeat step as necessary.)	(Domain Name attribute) Specifies the domain name that gets DNS resolution from the DNS server specified in Step 3. You can add multiple domain names to an open garden service.
Step 5	Router(config-prof)# exit	Returns to global configuration mode.
Step 6	Router(config)# ssg open-garden <i>profile-name</i>	Designates the service as an open garden service.

Example

In the following example, two services, called “nrp1-nrp2_og1” and “nrp1-nrp2_og1,” are defined and added to the open garden.

```
!
ssg open-garden nrp1-nrp2_og1
ssg open-garden nrp1-nrp2_og2
!
local-profile nrp1-nrp2_og1
  attribute 26 9 251 "Oopengarden1.com"
  attribute 26 9 251 "D10.13.1.5"
  attribute 26 9 251 "R10.1.1.0;255.255.255.0"
local-profile nrp1-nrp2_og2
  attribute 26 9 251 "Oopengarden2.com"
```



```

attribute 26 9 251 "D10.14.1.5"
attribute 26 9 251 "R10.2.1.0;255.255.255.0"
attribute 26 9 251 "R10.3.1.0;255.255.255.0"
!
```

Verifying the Open Garden Configuration

Use the **show ssg open-garden** privileged EXEC command to list all configured open garden services:

```

Router# show ssg open-garden
nrp1-nrp2_og1
nrp1-nrp2_og2
nrp1-nrp2_og3
nrp1-nrp2_og4
```

Monitoring and Troubleshooting Open Garden

Use the following commands to monitor and troubleshoot open garden services:

Command	Purpose
Router# clear ssg open-garden	Removes all instances of the ssg open-garden command from the configuration.
Router# clear ssg service profile-name	Removes the service object of the specified open garden service from the SSG service object table.
Router# show ssg open-garden	Lists all open garden services.
Router# show ssg service [service-name]	Displays detailed information about a service. If no service-name is entered, this command displays information for all services.

Examples

In the following example, all open garden services are displayed:

```

Router# show ssg open-garden
nrp1-nrp2_og110
nrp1-nrp2_og111
nrp1-nrp2_og112
nrp1-nrp2_og113
```

In the following example, detailed information is displayed for one of the open garden services:

```

Router# show ssg service nrp1-nrp2_og110

----- ServiceInfo Content -----
Uplink IDB: gw:0.0.0.0
Name:nrp1-nrp2_og110
Type:PASS-THROUGH
Mode:CONCURRENT
Service Session Timeout:0 seconds
Service Idle Timeout:0 seconds
Authentication Type:CHAP

DNS Server(s):Primary:10.13.1.5

Included Network Segments:
  10.1.1.0/255.255.255.0
```

```
Excluded Network Segments:
ConnectionCount 0
Full User Name not used
```

```
Domain List:opengarden110.com;
```

```
----- End of ServiceInfo Content -----
```

Configuring TCP Redirect - Logon



Note

Before configuring this feature, see the restrictions for TCP Redirect - Logon.

The TCP Redirect - Logon feature redirects certain packets, which would otherwise be dropped, to captive portals that can handle the packets in a suitable manner. For example, packets sent upstream by unauthorized users are forwarded to a captive portal that can redirect the users to a logon page. Similarly, if users try to access a service to which they have not logged on, the packets are redirected to a captive portal that can provide a service logon screen.

The captive portal can be any server that is programmed to respond to the redirected packets. If the Cisco SESM is used as a captive portal, subscribers are sent automatically to the SESM logon page when they start a browser session. The SESM captive portal application can also capture a URL in a subscriber's request and redirect the browser to the originally requested URL after successful authentication.

Redirected packets are always sent to a captive portal *group* that consists of one or more servers. SSG selects one server from the group in a round robin fashion to receive the redirected packets.

To configure the TCP Redirect - Logon feature, complete the following steps beginning in global configuration mode:

	Command	Purpose
Step 1*	<pre>Router(config)# ssg http-redirect group <i>groupname</i> server <i>ip-address port</i></pre> <p>(Repeat step as necessary.)</p>	<p>Defines a captive portal group. When the command is entered again with the same <i>groupname</i>, this command adds another server or port to that group. When entered with a unique <i>groupname</i>, this command defines a new captive portal group.</p>
Step 2	<pre>Router(config)# ssg http-redirect unauthorized-user group <i>groupname</i></pre>	<p>Specifies the default captive portal group where packets from unauthorized users are sent.</p>

Example

In the following example, two captive portal groups are defined: RedirectServer and SESMgroup. RedirectServer contains two servers with IP addresses 10.1.1.1 and 10.2.3.4 for the same TCP port 8080. SESMgroup contains one server at 10.1.1.1 for TCP port 8081. RedirectServer is specified as the default captive portal group where packets from unauthorized users are sent.

```
!
ssg http-redirect group RedirectServer server 10.1.1.1 8080
ssg http-redirect group RedirectServer server 10.2.3.4 8080
ssg http-redirect group SESMgroup server 10.1.1.1 8081
ssg http-redirect unauthorized-user group RedirectServer
!
```

Verifying TCP Redirect - Logon

Use the `show ssg http-redirect group` privileged EXEC command to:

- List all configured captive portal groups.
- Indicate which group is used for redirected packets from unauthorized users.

Monitoring and Troubleshooting TCP Redirect - Logon

Use the following commands to monitor and troubleshoot the TCP Redirect - Logon feature:

Command	Purpose
Router# <code>show ssg http-redirect group</code> [<i>groupname</i>]	Lists all configured captive portal groups and indicates which group receives redirected packets from unauthorized users. If the <i>groupname</i> is specified, this command displays detailed information about that captive portal group.
Router# <code>show ssg http-redirect mappings</code> [<i>ip-address</i>]	Displays the redirect mappings currently stored in SSG. If the host <i>ip-address</i> is provided, this command displays detailed redirect mapping information for the specified host.
Router# <code>debug ssg http-redirect</code>	Displays debug messages for the TCP Redirect - Logon feature.

Examples

In the following example, all configured captive portal groups are listed, and the unauthorized user redirect group is specified:

```
Router# show ssg http-redirect group
Current HTTP redirect groups:
  RedirectServer
  SESMgroup
Unauthorized user redirect group:RedirectServer
```

In the following example, detailed information is displayed about the RedirectServer and SESMgroup captive portal groups. Note, however, that redirectable destination networks and TCP ports are not supported in this release, so the last two lines of the following output are insignificant.

```
Router# show ssg http-redirect group RedirectServer
HTTP redirect group RedirectServer;
Showing all HTTP servers (Address, Port):
  10.1.1.1, 8080
  10.2.3.4, 8080
No redirectable destination networks defined.
No redirectable TCP ports defined.

Router# show ssg http-redirect group SESMgroup
HTTP redirect group SESMgroup;
Showing all HTTP servers (Address, Port):
  10.1.1.1, 8081
No redirectable destination networks defined.
No redirectable TCP ports defined.
```

In the following example, there are no redirect mappings currently stored in SSG:

```
Router# show ssg http-redirect mappings
No Http redirect mappings
```

In the following example, there are no redirect mappings currently stored in SSG for the user with IP address 10.8.8.7:

```
Router# show ssg http-redirect mappings 10.8.8.7
Host Address:10.8.8.7 has no stored redirect mappings
```

In the following example, all redirect mappings stored in SSG are displayed:

```
Router# show ssg http-redirect mappings
HTTP remapping Host:10.8.8.7 to server:10.1.1.1 on port:8080
HTTP remapping Host:10.8.8.8 to server:10.1.1.1 on port:8080
```

In the following example, detailed redirect mapping information is displayed for the user with IP address 10.8.8.7:

```
Router# show ssg http-redirect mappings 10.8.8.7
HTTP remapping Host:10.8.8.7 to server:10.1.1.1 on port:8080
Connection Mappings (src port <-> dest IP,dest port,timestamp,flags):
    1092 <-> 2.5.8.4,8080,1001321447,0x0
    1093 <-> 2.5.8.4,8080,1001321456,0x0
```

Configuring Host Key

Before configuring this feature, see the restrictions for Host Key.



Note

The SSG Host Key feature requires Cisco SSD Release 3.0(1) or Cisco SESM Release 3.1(1). If you are using an earlier release of SSD, disable the SSG Host Key feature with the **no ssg port-map enable** global configuration command.

To configure the SSG Host Key feature, complete the following tasks:

- Enabling the Host Key (Required if Currently Disabled)
- Specifying the Subscriber Traffic to be Port Mapped (Required)
- Specifying the SSG Source IP Addresses (Required)
- Specifying the Port-Bundle Length (Optional)



Note

All references to SESM also apply to SSD unless a clear distinction is made.

Enabling the Host Key (Required if Currently Disabled)

The host key is disabled by default. You can enable the host key by entering the following commands:

Command	Purpose
Router(config)# ssg port-map enable	Enables the host key.
Router# reload	You must reload the router for the previous command to take effect.

Example

```
ssg port-map enable
```

Specifying the Subscriber Traffic to be Port Mapped (Required)

The host key requires that you specify the subscriber traffic to be port mapped. SSG can compare the subscriber traffic against a configured TCP port range or an access list. SSG port maps the packets specified with one or both of the following global configuration commands:

Command	Purpose
Router(config)# ssg port-map destination range <i>port-number-1 to port-number-2 [ip ip-address]</i>	Specifies the TCP port range to compare against the subscriber traffic. Optionally specifies the destination IP address in the packets.
Router(config)# ssg port-map destination access-list <i>access-list-number</i>	Specifies an access list to compare against the subscriber traffic.



Note

You can use multiple entries of the **ssg port-map destination** commands. The port ranges and access lists are checked in the order in which they are defined.

Example

```
ssg port-map enable
ssg port-map destination range 8080 to 10100 ip 70.13.6.100
ssg port-map source ip Loopback1
```

Specifying the SSG Source IP Addresses (Required)

The Host Key feature requires that one or more SSG source IP addresses are specified for host key usage. One source IP address will permit the allocation of 4032 unique host keys, assuming a bundle length of 4 bits. For higher subscriber counts, configure additional addresses.



Note

All SSG source IP addresses configured with the **ssg port-map source ip** command must be routable in the management network where the SESM resides.

To specify SSG source IP addresses, use the following command in global configuration mode:

Command	Purpose
Router(config)# ssg port-map source ip { <i>ip-address</i> <i>interface</i> }	Specifies an SSG source IP address. If you specify an interface instead of an IP address, SSG uses the main IP address of the specified interface.



Note You can use multiple entries of the **ssg port-map source ip** commands.

Specifying the Port-Bundle Length (Optional)

The port-bundle length is used to determine the number of bundles in one group and the number of ports in one bundle. By default, the port-bundle length is 4 bits. The maximum port-bundle length is 10 bits. See Table 4-4 for available port-bundle length values, and the resulting port per bundle and bundle per group values. Increasing the port-bundle length can be useful when you see frequent error messages of running out of ports in a port bundle, but note that the new value does not take effect until the SSG next reloads, and SESM restarts.



Note For each SESM server, all connected SSGs must have the same port-bundle length, which must correspond to the configured value given in the SESM server's BUNDLE_LENGTH argument. If you change the port-bundle length on an SSG, be sure to make the corresponding change in the SESM configuration.

Table 4-4 Port-Bundle Lengths and Resulting Port per Bundle and Bundle per Group Values

Port-Bundle Length (in bits)	Number of Ports per Bundle	Number of Bundles per Group (and per SSG Source IP Address)
1	2	32256
2	4	16128
3	8	8064
4 (default)	16	4032
5	32	2016
6	64	1008
7	128	504
8	256	252
9	512	126
10	1024	63

To modify the port-bundle length upon the next SSG reload, enter the following command in global configuration mode:

Command	Purpose
Router(config)# ssg port-map length bits	(Takes effect upon next reload.) Modifies the port-bundle length, which is used to determine the number of ports per bundle and the number of bundles per group, as detailed in Table 4-4.

Verifying the Host Key

Step 1 To verify successful configuration of the SSG Host Key feature, enter the following command:

```
Router# show running-config
```

Step 2 To verify successful configuration of the SSG Host Key feature, enter the following command:

```
Router# show ssg port-map status
```

```
Bundle-length = 4
```

```
Bundle-groups:-
```

IP Address	Free Bundles	Reserved Bundles	In-use Bundles
70.13.60.2	4032	0	0

Monitoring and Troubleshooting SSG Host Key

Use the following commands to monitor and troubleshoot the SSG Host Key feature:

Command	Purpose
Router# show ssg port-map status [free reserved inuse]	Displays information on port-bundle groups, including: <ul style="list-style-type: none"> List of port-bundle groups Port-bundle length Number of free, reserved, and in-use port bundles in each group
Router# show ssg port-map ip ip-address port port-number	Displays the following information about a port bundle: <ul style="list-style-type: none"> Port maps in the port bundle Subscriber IP address Interface through which the subscriber is connected
Router# show ssg host ip-address interface	Displays the information about a subscriber and current connections of the subscriber.
Router# show ssg connection <i>ip-address interface service-name</i>	Displays the connections of a given host and a service name.
Router# clear ssg host ip-address interface	Removes or disables a given host or subscriber.
Router# clear ssg connection <i>ip-address interface service-name</i>	Removes the connections of a given host and a service name.

Command	Purpose
Router# <code>debug ssg port-map events</code>	Displays port mapping event messages.
Router# <code>debug ssg port-map packets</code>	Displays port mapping packet contents.

Examples

In the following examples, the interface Virtual-Access2 is connected to the subscriber:

```
Router# show ssg port-map status inuse
```

```
Bundle-group 70.13.60.2 has the following in-use port-bundles:-
```

Port-bundle	Subscriber Address	Interface
64	10.10.3.1	Virtual-Access2

```
Router# show ssg port-map ip 70.13.60.2 port 64
```

```
State = IN-USE
Subscriber Address = 10.10.3.1
Downlink Interface = Virtual-Access2
```

```
Port-mappings:-
```

Subscriber Port:	3271	Mapped Port:	1024
Subscriber Port:	3272	Mapped Port:	1025
Subscriber Port:	3273	Mapped Port:	1026
Subscriber Port:	3274	Mapped Port:	1027
Subscriber Port:	3275	Mapped Port:	1028

Configuring AAA Server Group Support for Proxy Services



Note

This section applies if you are using SSG with SSD or SESM in RADIUS mode.

This feature allows you to configure multiple AAA servers. You can configure each remote RADIUS server with timeout and retransmission parameters. SSG will perform failover among the servers in the predefined group.

To configure this feature, use the RADIUS Server attribute (described in Table 4-5) to enter the remote server information into the proxy service profile. SSG automatically creates a AAA server group that contains the remote RADIUS server for this service profile.

Table 4-5 Service-Info VSA Used to Configure AAA Server Group Support for Proxy Services

Attribute	Usage
RADIUS Server	(Required for proxy services) Specifies the remote RADIUS servers that the SSG uses to authenticate and authorize a service log on for a proxy service type.

For detailed information on this Service-Info VSA, see the “Service Profiles” section on page 4-46. For general information on configuring RADIUS profiles for SSG, see the “Configuring RADIUS Profiles” section on page 4-39.

Verifying the AAA Server Groups for Proxy Radius

To display the AAA server group information, enter the **show ssg service** privileged EXEC command.

```
Router# show ssg service serv1-proxy
```

Configuring the Proxy RADIUS Enhancements



Note

This section applies if you are using SSG with SSD or SESM in RADIUS mode.

Before configuring this feature, see the restrictions for Proxy RADIUS Enhancements.

This feature introduces the Service-Info VSAs described in Table 4-6.

Table 4-6 Service-Info VSAs Introduced by the Proxy RADIUS Enhancements

Attribute	Usage
Full Username Attribute	Enables usage of the full username (user@service) in the RADIUS authentication and accounting requests.
Service-Defined Cookie	Allows user-defined information to be included in the RADIUS authentication and accounting requests.

For detailed information on these Service-Info VSAs, see the “Service Profiles” section on page 4-46. For general information on configuring RADIUS profiles for SSG, see the “Configuring RADIUS Profiles” section on page 4-39.

Example: Proxy RADIUS Enhancements

The following proxy RADIUS service profile contains a Service-Defined Cookie and a Full Username Attribute:

```
user = serv1-proxy{
  profile_id = 98
  profile_cycle = 42
  member = Single_Logon
  radius=6510-SSG-v1.1a {
    check_items= {
      2=alex
    }
    reply_attributes= {
      9,251="Oservice1.com"
      9,251="R10.13.0.0;255.255.0.0"
      9,251="TX"
      9,251="D10.13.1.5"
      9,251="S10.13.1.2;1645;1646;my-secret"
      9,251="Gmy-key"
      → 9,251="X"
      → 9,251="Vproxy-service_at_X.X.X.X"
    }
  }
}
```

Verifying the Proxy RADIUS Enhancements

- Step 1** To verify that the new Service-Info attributes exist in the proxy RADIUS service profile, enter the **show ssg service service-name** command and check for the “Full User Name Used” and “Service Defined Cookie exist” statements in the output.

```

Router# show ssg service serv1-proxy
----- ServiceInfo Content -----
Uplink IDB:
Name:serv1-proxy
Type:PROXY
Mode:CONCURRENT
Service Session Timeout:0 seconds
Service Idle Timeout:0 seconds
Class Attr:NONE
Authentication Type:CHAP
Reference Count:1

Next Hop Gateway Key:my-key

DNS Server(s):Primary:10.13.1.5

Radius Server:IP=10.13.1.2, authPort=1645, acctPort=1646, secret=my-secret

Included Network Segments:
    10.13.0.0/255.255.0.0
Excluded Network Segments:
→ Full User Name Used
→ Service Defined Cookie exist

Domain List:servicel.com;

Active Connections:
    1 :Virtual=255.255.255.255, Subscriber=10.20.10.2

----- End of ServiceInfo Content -----

```

- Step 2** To check the content of the RADIUS profiles, refer to the user documentation for your RADIUS server.

RADIUS Accounting Records



Note

This section applies if you are using SSG with SSD or SESM in RADIUS or DESS mode.

This section describes events that generate RADIUS accounting records and the attributes associated with the accounting records sent from the SSG to the accounting server.

Account Logon

When a user logs in, the SSG sends a RADIUS accounting-request on behalf of the user to the accounting server. The attributes associated with this record are:

```
Acct-Status-Type = Start
NAS-IP-Address = ip_address
User-Name = "username"
Acct-Session-Id = "session_id"
Framed-IP-Address = user_ip
Proxy-State = "n"
```

<i>ip_address</i>	IP address of the SSG.
<i>username</i>	Name used to log in to the service provider network.
<i>session_id</i>	Session number.
<i>user_ip</i>	IP address of the user's system.
<i>n</i>	Accounting record queuing information (has no effect on account billing).

Account Logoff

When a user logs off, the SSG sends a RADIUS accounting-request on behalf of the user to the accounting server. The attributes associated with this record are:

```
Acct-Status-Type = Stop
NAS-IP-Address = ip_address
User-Name = "username"
Acct-Session-Time = time
Acct-Terminate-Cause = cause
Acct-Session-Id = "session_id"
Framed-Address = user_ip
Proxy-State = "n"
```

<i>ip_address</i>	IP address of the SSG.
<i>username</i>	Name used to log on to the service provider network.
<i>time</i>	Length of session in seconds.
<i>cause</i>	Cause of account termination. These can include: <ul style="list-style-type: none"> • User-Request. • Session-Timeout. • Idle-Timeout. • Lost-Carrier.
<i>session_id</i>	Session number.
<i>user_ip</i>	IP address of the user's system.
<i>n</i>	Accounting record queuing information (has no effect on account billing).

Connection Start

When a user accesses a service, the SSG sends a RADIUS accounting-request to the accounting server. The attributes associated with this record are:

```
NAS-IP-Address = 172.16.6.1
NAS-Port = 0
NAS-Port-Type = Virtual
User-Name = "username"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "00000010"
Framed-Protocol = PPP
Service-Info = "Nisp-name.com"
Service-Info = "Username"
Service-Info = "TP"
Acct-Delay-Time = 0
```

<i>ip_address</i>	IP address of the SSG.
<i>username</i>	Name used to log on to the service provider network.
<i>session_id</i>	Session number.
<i>service</i>	Name of the service profile.
<i>hg_username</i>	The username used to authenticate the user with the remote RADIUS server. This attribute is used for proxy services.
<i>type</i>	X—Proxy connection. P—Passthrough connection (usually the Internet).
<i>n</i>	Accounting record queuing information (has no effect on account billing).

Connection Stop

When a user terminates a service, the SSG sends a RADIUS accounting-request to the accounting server. The attributes associated with this record are:

```
NAS-IP-Address = 192.168.2.48
NAS-Port = 0
NAS-Port-Type = Virtual
User-Name = "zeus"
Acct-Status-Type = Stop
Service-Type = Framed-User
Acct-Session-Id = "00000002"
Acct-Terminate-Cause = User-Request
Acct-Session-Time = 84
Acct-Input-Octets = 0
Acct-Output-Octets = 649
Acct-Input-Packets = 0
Acct-Output-Packets = 17
Framed-Protocol = PPP
Framed-IP-Address = 201.168.101.10
Control-Info = "I0;0"
Control-Info = "O0;649"
Service-Info = "Ninternet"
Service-Info = "Uzeus"
Service-Info = "TP"
Acct-Delay-Time = 0
```

<i>ip_address</i>	IP address of the SSG.
<i>username</i>	Name used to log on to the service provider network.
<i>in_bytes</i>	Number of inbound bytes.
<i>out_bytes</i>	Number of outbound bytes.
<i>time</i>	Length of session in seconds.
<i>cause</i>	Cause of service termination. These include: <ul style="list-style-type: none"> • User-Request. • Lost-Carrier. • Lost-Service. • Session-Timeout. • Idle-Timeout.
<i>session_id</i>	Session number.
<i>service</i>	Name of the service profile.
<i>hg_username</i>	The username used to authenticate the user with the remote RADIUS server. This attribute is used for proxy services.
<i>type</i>	X—Proxy connection. P—Passthrough connection (usually the Internet).
<i>n</i>	Accounting record queuing information (has no effect on account billing).

Attributes Used in Accounting Records

Service User

This attribute indicates the username provided by the SESM user to log on to the service and for authentication with the home gateway.

Service-Info = "Username"

Syntax Description

username The name provided by the user for authentication.

Example

```
Service-Info = "Ujoe@cisco.com"
```



Note

This attribute is only used for accounting purposes and does not appear in profiles.

Service Name

This attribute defines the name of the service.

Service-Info = "Nname"

Syntax Description

name Name of the service profile or service that belongs to a service group.

Example

```
Service-Info = "Nservice1.com"
```



Note

This attribute is only used for accounting purposes and does not appear in profiles.

Octets Output

Current RADIUS standards only support the counting of up to 32 bits of information with the ACCT-Output-Octets attribute. Standards such as ADSL have much higher throughput.

In order for the accounting server to keep track of and bill for this usage, the SSG uses the Octets attribute.

The Octets Output attribute keeps track of how many times the 32-bit integer rolled over and the value of the integer when it overflowed for outbound data.

Control-Info = "Orollover;value"

Syntax Description

rollover Number of times the 32-bit integer rolled over to 0.

value Value in the 32-bit integer when the stop record was generated and the service or user was logged out.

Usage

Use this attribute to accurately keep track of and bill for usage. To calculate the actual number of bytes, use the following formula:

$$\text{rollover} * 2^{32} + \text{value}$$

Example

In the following example, the rollover is 2 and the value is 153 ($2 * 2^{32} + 153 = 8589934745$):

```
Control-Info = "02;153"
```



Note

This attribute is only used for accounting purposes and does not appear in profiles.

Octets Input

Current RADIUS standards only support the counting of up to 32 bits of information with the ACCT-Input-Octets attribute. Standards such as ADSL have much higher throughput.

In order for the accounting server to keep track of and bill for this usage, the SSG uses the Octets attribute.

The Octets Input attribute keeps track of how many times the 32-bit integer rolled over and the value of the integer when it overflowed for inbound data.

Control-Info = "Irollover;value"

Syntax Description

<i>rollover</i>	Number of times the 32-bit integer rolled over to 0.
<i>value</i>	Value in the 32-bit integer when the stop record was generated and the service or user was logged out.

Usage

Use this attribute to accurately keep track of and bill for usage. To calculate the actual number of bytes, use the following formula:

$$\text{rollover} * 2^{32} + \text{value}$$

Example

In the following example, the rollover is 3 and the value is 151 ($3 * 2^{32} + 151 = 12884902039$):

```
Control-Info = "I3;151"
```



Note

This attribute is only used for accounting purposes and does not appear in profiles.

Configuring RADIUS Profiles



Note

This section applies if you are using SSG with SESM in RADIUS mode or with SSD.

If you are using SSG with SESM in DESS mode, see the *Cisco Distributed Administration Tool Guide* for information on creating and maintaining subscriber, service, and policy information in an LDAP directory, including defining a tunnel service profile.

The SSG uses vendor-specific RADIUS attributes to define RADIUS profiles. You must customize the AAA server's RADIUS dictionary to incorporate the SSG vendor-specific attributes described in SSG Vendor-Specific Attributes.

You must set up user and service RADIUS profiles on the AAA server as described in this section. Service profiles can also be defined locally as described in the "Configuring Local Service Profiles" section. You can optionally set up pseudo-service profiles. The following profiles are described:

- User Profiles
- Service Profiles
- Service Group Profiles
- Pseudo-Service Profiles

These profiles contain RADIUS attributes that define specific AAA elements. The syntax for these attributes is described in this section.

SSG Vendor-Specific Attributes

Table 4-7 lists vendor-specific attributes used by the SSG. By sending an Access-Request packet with the vendor-specific attributes shown in the table, the SESM can send requests to the SSG to log in and log off an account and disconnect and connect services. The vendor ID for all of the Cisco-specific attributes is 9.

Table 4-7 Vendor-Specific RADIUS Attributes for the SSG

AttrID	VendorID	SubAttrID	SubAttrName	SubAttrDataType
26	9	1	Cisco-AVpair	String
26	9	250	Account-Info	String
26	9	251	Service-Info	String
26	9	253	Control-Info	String

The following sections describe the format of each subattribute.



Note

All RADIUS attributes are case sensitive.

Cisco-AVpair Attributes

The Cisco-AVpair attributes are used in user and service profiles to configure access control lists (ACLs) and Layer 2 Tunnel Protocol (L2TP).

Table 4-8 Cisco-AVPair Attributes

Attribute	Usage
Downstream Access Control List (outacl)	Specifies either an IOS standard access control list or an extended access control list to be applied to downstream traffic going to the user.
L2TP Tunnel Password	Specifies the secret (password) used for L2TP tunnel authentication.
Upstream Access Control List (inacl)	Specifies either an IOS standard access control list or an extended access control list to be applied to upstream traffic coming from the user.
VPDN IP Address	Specifies the IP addresses of the home gateways (LNSes) to receive the L2TP connections.
VPDN Tunnel ID	Specifies the name of the tunnel that must match the tunnel ID specified in the LNS VPDN group.

Account-Info Attributes

The Account-Info attributes are used in user profiles and service group profiles.

User profiles define the password, services, and groups to which the user is subscribed.

Service group profiles contain a list of services and service groups and can be used to create sophisticated directory structures for locating and logging in to services. When a user is subscribed to a service group, the user is automatically subscribed to all services and groups within that service group. A service group profile includes the name of the service group, the password, the service type (outbound), a list of services and/or a list of other service groups.

Example (RADIUS Freeware Format)

```
Account-Info = "Nservice1.com"
```

Example (CiscoSecure ACS for UNIX Format)

```
9,250 = "Nservice1.com"
```

Table 4-9 Account-Info Attributes

Attribute	Usage
Auto Service	Automatically logs a user into a service when the user logs on to the SSG (reply attribute).
Group Description	Provides a description of the service group.
Home URL	(Optional) The URL for the user's preferred Internet home page.
Service Group	Subscribes the user to a service group. There can be multiple instances of this attribute within a single user profile. Use one attribute for each service group to which the user is subscribed (reply attribute).
Service Name	Subscribes the user to a service. There can be multiple instances of this attribute within a single user profile. Use one attribute for each service to which the user is subscribed (reply attribute).

Service-Info Attributes

The Service-Info attributes are used to define a service. The following attributes define the parameters for a service.

Table 4-10 Service-Info Attributes

Attribute	Usage
DNS Server Address	(Optional) Specifies the primary and secondary DNS servers for this service.
Domain Name	(Optional) Specifies domain names that get DNS resolution from the DNS server(s) specified in DNS Server Address.
Full Username Attribute	Enables usage of the full username (user@service) in the RADIUS authentication and accounting requests.
MTU Size	Specifies the PPP MTU size of the SSG as an L2TP access concentrator (LAC). By default, the PPP MTU size is 1500 bytes. Note SESM in DESS mode does not support use of this attribute.

Table 4-10 Service-Info Attributes (continued)

Attribute	Usage
RADIUS Server	(Required for proxy services) Specifies the remote RADIUS server that the SSG uses to authenticate and authorize a service log on for a proxy service type.
Service-Defined Cookie	Allows user-defined information to be included in the RADIUS authentication and accounting requests.
Service Description	(Optional) Provides a description of the service that is displayed to the user.
Service Mode	(Optional) Specifies whether the user is able to log on to this service while simultaneously connected to other services (concurrent) or whether the user cannot access any other services while using this service (sequential). The default is concurrent.
Service Name	Defines the name of the service.
Service Next Hop Gateway	(Optional) Specifies the next hop key for this service. Each SSG uses its own next hop gateway table that associates this key with an actual IP address. For information on creating a next hop gateway table, see the “Next Hop Gateway Pseudo-Service Profile” section.
Service Route	(Required) Specifies networks that exist for the service. There can be multiple instances of this attribute within a single user profile.
Service URL	(Optional) The URL displayed in the SESM HTTP address field when the service opens.
Service User	Indicates the username provided by the SESM user to log on to the service and for authentication with the home gateway.
Type of Service	(Optional) Indicates whether the service is proxy (requiring remote authentication) or passthrough (does not require authentication). The default is passthrough.

Control-Info Attributes

The Control-Info attribute is used to define lists or tables of information.

Table 4-11 Control-Info Attribute

Attribute	Usage
Next Hop Gateway Table Entry	Associates next hop gateway keys with IP addresses.

User Profiles

RADIUS user profiles contain a password, a list of subscribed services and groups, and access control lists.

Table 4-12 describes attributes that appear in RADIUS user profiles.

Table 4-12 User Profile Attributes

Attribute	Usage
Cisco-AVPair Attributes	
Downstream Access Control List (outacl)	Specifies either an IOS standard access control list or an extended access control list to be applied to downstream traffic going to the user.
Upstream Access Control List (inacl)	Specifies either an IOS standard access control list or an extended access control list to be applied to upstream traffic coming from the user.
Account-Info Attributes	
Auto Service	Automatically logs a user into a service when the user logs on to the SSG (reply attribute).
Home URL	(Optional) The URL for the user's preferred Internet home page.
Service Group	Subscribes the user to a service group. There can be multiple instances of this attribute within a single user profile. Use one attribute for each service group to which the user is subscribed (reply attribute).
Service Name	Subscribes the user to a service. There can be multiple instances of this attribute within a single user profile. Use one attribute for each service to which the user is subscribed (reply attribute).
Standard Attributes¹	
Idle-Timeout	Specifies, in seconds, the maximum time a connection can remain idle (reply attribute).
Password	Specifies the user's password (check attribute).
Session-Timeout	Specifies, in seconds, the maximum length of the user's session (reply attribute).

1. Standard attributes are described in detail in RFC2138.

Downstream Access Control List

This attribute specifies either an IOS standard access control list or an extended access control list to be applied to downstream traffic going to the user.

Cisco-AVpair = "ip:outacl[#number]={*standard-access-control-list* | *extended-access-control-list*}"

Syntax Description

number Access list identifier.
standard-access-control-list Standard access control list.
extended-access-control-list Extended access control list.

Example

```
Cisco-AVpair="ip:outacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21"
```

**Note**

There can be multiple instances of this attribute within profiles. Use one attribute for each access control list statement. Multiple attributes can be used for the same ACL. Multiple attributes are downloaded according to the number specified and executed in that order.

Upstream Access Control List

This attribute specifies either an IOS standard access control list or an extended access control list to be applied to upstream traffic coming from the user.

Cisco-AVpair = "ip:inacl[#number]={standard-access-control-list | extended-access-control-list}"

Syntax Description

number Access list identifier.
standard-access-control-list Standard access control list.
extended-access-control-list Extended access control list.

Example

```
Cisco-AVpair="ip:inacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21"
```

**Note**

There can be multiple instances of this attribute within profiles. Use one attribute for each access control list statement. Multiple attributes can be used for the same ACL. Multiple attributes are downloaded according to the number specified and executed in that order.

Auto Service

This attribute subscribes the user to a service and automatically logs the user on to the service when the user accesses SESM. Each user profile can have more than one auto service attribute.

Account-Info = "Aservicename [;username;password]"

Syntax Description

servicename Name of the service.
username Username used to access the service. Required for proxy services.
password Password used to access the service. Required for proxy services.

Example

```
Account-Info = "Agamers.net;jdoe;secret"
```

**Note**

The user must be subscribed to this service. See "Auto Service".

Home URL

This attribute specifies the URL for the user's preferred Internet home page. This attribute is optional.

Account-Info = "**H**url"

or

Account-Info = "**U**url"

Syntax Description

url A fully qualified URL for the user's preferred Internet home page.

Usage

If the SESM web application is designed to use HTML frames, then this attribute also specifies whether the home page is displayed in a new browser window or in a frame in the current (SESM) window, as follows:

- **Hurl**—URL for the home page displayed in a frame in the SESM browser window.
- **Uurl**—URL for the home page displayed in its own browser window.



Note

In a frameless application, both **H** and **U** cause a new browser window to open for the home page. The NWSP application is a frameless application.

Example

```
Account-Info = "Uhttp://www.BestVideo.com"
```

Service Group

In user profiles, this attribute subscribes a user to a service group. In service group profiles, this attribute lists the service subgroups that belong to this service group.

Account-Info = "**G**name"

Syntax Description

name Name of the group profile.

Example

```
Account-Info = "GServiceGroup1"
```



Note

There can be multiple instances of this attribute within a user or service group profile. Use one attribute for each service subgroup.

Service Name

In user profiles, this attribute subscribes the user to the specified service. In service group profiles, this attribute lists services that belong to the service group.

Account-Info = "Nname"

Syntax Description

name Name of the service profile.

Example (RADIUS Freeware Format)

```
Account-Info = "Ncisco.com"
```

Example (CiscoSecure ACS for UNIX)

```
9,250="cisco.com"
```



Note There can be multiple instances of this attribute within a user or service profile. Use one attribute for each service.

Example User Profile

The following is an example of a user profile. The profile is formatted for use with a freeware RADIUS server:

```
bert Password = "ernie"
Session-Timeout = 21600,
Account-Info = "GServiceGroup1",
Account-Info = "Nservice1.com",
Account-Info = "Ngamers.net"
```

The following is the same profile as above, formatted for CiscoSecure ACS for UNIX:

```
user = bert {
radius = SSG {
check_items = {
2 = "ernie"
}
reply_attributes = {
27 = 21600
9,250 = "GServiceGroup1"
9,250 = "Nservice1.com"
9,250 = "Ngamers.net"
}
}
}
```

Service Profiles

Service profiles include the password, service type (outbound), type of service (passthrough or proxy), the service access mode (sequential or concurrent), the DNS server IP address, networks that exist in the service domain, access control lists, and other optional attributes.

Table 4-13 describes attributes that appear in RADIUS service profiles.

Table 4-13 Service Profile Attributes

Attribute	Usage
Cisco-AVPair Attributes	
Downstream Access Control List (outacl)	Specifies either an IOS standard access control list or an extended access control list to be applied to downstream traffic going to the user.
Upstream Access Control List (inacl)	Specifies either an IOS standard access control list or an extended access control list to be applied to upstream traffic coming from the user.
L2TP Tunnel Password	Specifies the secret (password) used for L2TP tunnel authentication.
VPDN IP Address	Specifies the IP addresses of the home gateways (LNSes) to receive the L2TP connections.
VPDN Tunnel ID	Specifies the name of the tunnel that must match the tunnel ID specified in the LNS VPDN group.
Service-Info Attributes	
DNS Server Address	(Optional) Specifies the primary and/or secondary DNS servers for this service.
Domain Name	(Optional) Specifies domain names that get DNS resolution from the DNS server(s) specified in DNS Server Address.
Full Username Attribute	Enables usage of the full username (user@service) in the RADIUS authentication and accounting requests.
MTU Size	Specifies the PPP MTU size of the SSG as an L2TP access concentrator (LAC). By default, the PPP MTU size is 1500 bytes. Note SESM in DESS mode does not support use of this attribute.
RADIUS Server	(Required for proxy services) Specifies the remote RADIUS servers that the SSG uses to authenticate and authorize a service log on for a proxy service type.
Service Authentication Type	Specifies whether the SSG uses the CHAP or PAP protocol to authenticate users for proxy services.
Service-Defined Cookie	Allows user-defined information to be included in the RADIUS authentication and accounting requests.
Service Description	(Optional) Provides a description of the service that is displayed to the user.
Service Mode	(Optional) Specifies whether the user is able to log on to this service while simultaneously connected to other services (concurrent) or whether the user cannot access any other services while using this service (sequential). The default is concurrent.

Table 4-13 Service Profile Attributes (continued)

Attribute	Usage
Service Next Hop Gateway	(Optional) Specifies the next hop key for this service. Each SSG uses its own next hop gateway table that associates this key with an actual IP address. For information on creating a next hop gateway table, see “Next Hop Gateway Pseudo-Service Profile”.
Service Route	(Required) Specifies networks that exist for the service. There can be multiple instances of this attribute within a single user profile.
Service URL	(Optional) The URL displayed in the SESM HTTP address field when the service opens.
Type of Service	(Optional) Indicates whether the service is proxy (requiring remote authentication) or passthrough (does not require authentication). The default is passthrough.
Standard Attributes¹	
Idle-Timeout	Specifies, in seconds, the maximum time a service connection can remain idle (reply attribute).
Password	Specifies the password (check attribute).
Session-Timeout	Specifies, in seconds, the maximum length of the session (reply attribute).
Service-Type	Specifies the level of service (check attribute). Must be “outbound.”

1. Standard attributes are described in detail in RFC2138.

Downstream Access Control List

This attribute specifies either an IOS standard access control list or an extended access control list to be applied to downstream traffic going to the user.

Cisco-AVpair = “ip:outacl[#number]={standard-access-control-list | extended-access-control-list}”

Syntax Description

<i>number</i>	Access list identifier.
<i>standard-access-control-list</i>	Standard access control list.
<i>extended-access-control-list</i>	Extended access control list.

Example

```
Cisco-AVpair="ip:outacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21"
```



Note There can be multiple instances of this attribute within profiles. Use one attribute for each access control list statement. Multiple attributes can be used for the same ACL. Multiple attributes are downloaded according to the number specified and executed in that order.

Upstream Access Control List

This attribute specifies either an IOS standard access control list or an extended access control list to be applied to upstream traffic coming from the user.

Cisco-AVpair = "ip:inacl[#number]={standard-access-control-list | extended-access-control-list}"

Syntax Description

<i>number</i>	Access list identifier.
<i>standard-access-control-list</i>	Standard access control list.
<i>extended-access-control-list</i>	Extended access control list.

Example

```
Cisco-AVpair="ip:inacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21"
```



Note There can be multiple instances of this attribute within profiles. Use one attribute for each access control list statement. Multiple attributes can be used for the same ACL. Multiple attributes are downloaded according to the number specified and executed in that order.

L2TP Tunnel Password

This attribute is the secret (password) used for L2TP tunnel authentication.

Cisco-AVpair = "vpdn:tunnel-password=*secret*"

Syntax Description

<i>secret</i>	Secret (password) for L2TP tunnel authentication.
---------------	---

Example (RADIUS Freeware Format)

```
Cisco-AVpair="vpdn:l2tp-tunnel-password=cisco"
```

Example (CiscoSecure ACS for UNIX)

```
9,1="vpdn:l2tp-tunnel-password=cisco"
```

VPDN IP Address

This attribute specifies the IP addresses of the home gateways (LNSes) to receive the L2TP connections.

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

Syntax Description

<i>address</i>	IP address of the home gateway.
----------------	---------------------------------

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

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, 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 Tunnel ID

This attribute specifies the name of the tunnel that must match the tunnel ID specified in the LNS VPDN group, as shown in Step 4 in the “Configuring the LNS” section on page 4-21.

Cisco-AVpair = "vpdn:tunnel-id=*name*"

Syntax Description

<i>name</i>	Tunnel name.
-------------	--------------

Example (RADIUS Freeware Format)

```
Cisco-AVpair="vpdn:tunnel-id=My-Tunnel"
```

Example (CiscoSecure ACS for UNIX)

```
9,1="vpdn:tunnel-id=My-Tunnel"
```

DNS Server Address

This attribute specifies the primary and secondary DNS servers for this service. If two servers are specified, the SSG can send DNS requests to the primary DNS server until performance is diminished or it fails (failover). This attribute is optional.

Service-Info = "D*ip_address_1*[:*ip_address_2*]"

Syntax Description

<i>ip_address_1</i>	IP address of the primary DNS server.
<i>ip_address_2</i>	(Optional) IP address of the secondary DNS server used for fault tolerance.

Example

```
Service-Info = "D192.168.1.2;192.168.1.3"
```

Domain Name

This attribute specifies domain names that get DNS resolution from the DNS server(s) specified in DNS server address. This attribute is optional.

Service-Info = "Oname1[;name2]...[;nameX]"

Syntax Description

<i>name1</i>	Domain name that gets DNS resolution from this server.
<i>name2...X</i>	(Optional) Additional domain name(s) that gets DNS resolution from this server.

Usage

Use the DNS Resolution attribute to specify domain names that get DNS resolution from this DNS server. For more information, see "Service Access Order".

Example

```
Service-Info = "Ocisisco.com;cisco-sales.com"
```



Note

There can be multiple instances of this attribute within a single service profile.

Full Username Attribute

This attribute indicates that the RADIUS authentication and accounting requests use the full username (user@service).

Service-Info = "X"

The size of the full username is limited to the smaller of the following values:

- 246 bytes (10 bytes less than the standard RADIUS protocol limitation)
- *Max* - 10 bytes, where *Max* is the maximum size of the RADIUS attribute supported by your proxy RADIUS server

Example (RADIUS Freeware Format)

```
Service-Info = "X"
```

Example (CiscoSecure ACS for UNIX)

```
9,251="X"
```

MTU Size



Note

SESM in DESS mode does not support use of this attribute.

This attribute specifies the PPP MTU size of the SSG as a LAC. By default, the PPP MTU size is 1500 bytes.

Service-Info = "Bsize"

Syntax Description

<i>size</i>	MTU size in bytes
-------------	-------------------

Example (RADIUS Freeware Format)

```
9,251="B1500"
```

Example (CiscoSecure ACS for UNIX)

```
9,1="B1500"
```

RADIUS Server

This attribute specifies the remote RADIUS servers that the SSG uses to authenticate, authorize, and perform accounting for a service log on for a proxy service type. This attribute is only used in proxy service profiles and is required.

You can configure each remote RADIUS server with timeout and retransmission parameters. SSG will perform failover among the servers.

Service-Info =

“SRadius-server-address;auth-port;acct-port;secret-key[;retrans;timeout;deadtime]”

Syntax Description

<i>Radius-server-address</i>	IP address of the RADIUS server.
<i>auth-port</i>	UDP port number for authentication and authorization requests.
<i>acct-port</i>	UDP port number for accounting requests.
<i>secret-key</i>	Secret key shared with RADIUS clients.
<i>retrans</i>	Number of retransmissions. Default is 3.
<i>timeout</i>	Time in seconds before retransmission. Default is 5.
<i>deadtime</i>	Time in minutes during which the SSG will not try to perform authentication or accounting with a AAA server that was detected as down. Default is 10.

Example

```
Service-Info = "S192.168.1.1;1645;1646;cisco"
```

Service Authentication Type

This attribute specifies whether the SSG uses the CHAP or PAP protocol to authenticate users for proxy services.

Service-Info = "Aauthen-type"**Syntax Description**

<i>authen-type</i>	C—CHAP Authentication. P—PAP Authentication.
--------------------	---

Example

```
Service-Info = "AC"
```

Service-Defined Cookie

This attribute enables you to include user defined information in the RADIUS authentication and accounting requests.

Service-Info = “Vstring”

Syntax Description

<i>string</i>	Information of your choice that you wish to include in the RADIUS authentication and accounting requests. The size of the user-defined <i>string</i> is limited to the smaller of the following values: <ul style="list-style-type: none"> • 246 bytes (10 bytes less than the standard RADIUS protocol limitation) • <i>Max</i> - 10 bytes, where <i>Max</i> is the maximum size of the RADIUS attribute supported by your proxy RADIUS server
---------------	--

Example (RADIUS Freeware Format)

```
Service-Info = "VserviceIDandAAA-ID"
```

Example (CiscoSecure ACS for UNIX)

```
9,251="VserviceIDandAAA-ID"
```

**Note**

SSG does not parse or interpret the value of the Service-Defined Cookie. You must configure the proxy RADIUS server to interpret this attribute.

**Note**

SSG supports only one Service-Defined Cookie per RADIUS service profile.

Service Description

This attribute describes the service. This attribute is optional.

Service-Info = “Idescription”

Syntax Description

<i>description</i>	Description of the service.
--------------------	-----------------------------

Example

```
Service-Info = "ICompany Intranet Access"
```

Service Mode

This attribute defines whether the user is able to log on to this service while simultaneously connected to other services (concurrent) or whether the user cannot access any other services while using this service (sequential). The default is concurrent. This attribute is optional.

Service-Info = “Mmode”

Syntax Description

mode S—Sequential mode.
 C—Concurrent mode. This is the default.

Example

```
Service-Info = "MS"
```

Service Next Hop Gateway

This attribute specifies the next hop key for this service. Each SSG uses its own next hop gateway table that associates this key with an actual IP address. For information on creating a next hop gateway table, see “Next Hop Gateway Table Entry”. This attribute is optional.

Service-Info = “Gkey”

Syntax Description

key Name of the next hop.

Example

```
Service-Info = "Gnexthop1"
```

Service Route

This attribute specifies networks available to the user for this service. This attribute is required.

Service-Info = “Rip_address;mask”

Syntax Description

ip_address IP address.
mask Subnet mask.

Usage

Use the Service Route attribute to specify networks that exist for a service. For more information, see “Service Access Order”.



Note

An Internet service is typically specified as "R0.0.0.0;0.0.0.0" in the service profile.

Example

```
Service-Info = "R192.168.1.128;255.255.255.192"
```

**Note**

There can be multiple instances of this attribute within a single service profile.

Service URL

This attribute specifies the URL that is displayed in the SESM HTTP address field when the service opens. This attribute is optional.

Service-Info = "Hurl"

or

Service-Info = "Uurl"

Syntax Description

<i>url</i>	A fully qualified URL that is displayed in the SESM HTTP address field when the service opens.
------------	--

Usage

If the SESM web application is designed to use HTML frames, then this attribute also specifies whether the service is displayed in a new browser window or in a frame in the current (SESM) window, as follows:

- **Hurl**—URL for a service displayed in a frame in the SESM browser window.
- **Uurl**—URL for a service displayed in its own browser window.

**Note**

In a frameless application, both **H** and **U** cause a new browser window to open for the service. The NWSP application is a frameless application.

Example

```
Service-Info = "Uhttp://www.BestVideo.com"
```

Type of Service

This attribute indicates whether the service is proxy, tunnel, or passthrough. This attribute is optional.

Service-Info = "Ttype"

Syntax Description

<i>type</i>	<p>P—Passthrough. Indicates the user's packets are forwarded through the SSG. This is the default.</p> <p>T—Tunnel. Indicates that this is a tunneled service.</p> <p>X—Proxy. Indicates the SSG performs proxy service.</p>
-------------	---

Example (RADIUS Freeware Format)

```
Service-Info = "TT"
```

Example (CiscoSecure ACS for UNIX)

```
9,251="TT"
```

Example Service Profile

The following is an example of a service profile. The profile is formatted for use with a freeware RADIUS server:

```
service1.com Password = "cisco", Service-Type = outbound,
Idle-Timeout = 1800,
Service-Info = "R192.168.1.128;255.255.255.192",
Service-Info = "R192.168.2.0;255.255.255.192",
Service-Info = "R192.168.3.0;255.255.255.0",
Service-Info = "Gservice1",
Service-Info = "D192.168.2.81",
Service-Info = "MC",
Service-Info = "TP",
Service-Info = "ICompany Intranet Access",
Service-Info = "Oservice1.com"
```

The following is the same profile as above, formatted for CiscoSecure ACS for UNIX:

```
user = service1.com {
radius = SSG {
check_items = {
2 = "cisco"
6 = 5
}
reply_attributes = {
28 = 1800
9,251 = "R192.168.1.128;255.255.255.192"
9,251 = "R192.168.2.0;255.255.255.192"
9,251 = "R192.168.3.0;255.255.255.0"
9,251 = "Gservice1"
9,251 = "D192.168.2.81"
9,251 = "MC"
9,251 = "TP"
9,251 = "ICompany Intranet Access"
9,251 = "Oservice1.com"
}
}
}
```

Service Group Profiles

Service group profiles contain a list of services and service groups and can be used to create directory structures for locating and logging on to services. When a user is subscribed to a service group, the user automatically is subscribed to all services and groups within that service group. A service group profile includes the password and the service type (outbound) as check attributes and a list of services and a list of service groups as reply attributes.

Table 4-14 describes attributes that can be used in SSG service group profiles.

Table 4-14 Service Group Profile Attributes

Attribute	Usage
Account-Info Attributes	
Group Description	Provides a description of the service group.
Service Name	Lists services that belong to the service group. There can be multiple instances of this attribute within a single user profile. Use one attribute for each service (reply attribute).
Service Group	Lists the service subgroups that belong to this service group. When configured, the service group and service name attributes can define an organized directory structure for accessing services. There can be multiple instances of this attribute within a service group profile. Use one attribute for each service subgroup that belongs to this service group.
Standard Attributes¹	
Password	Specifies the password (check attribute).
Service-Type	Specifies the level of service (check attribute). Must be "outbound."

1. Standard attributes are described in detail in RFC2138.

Group Description

This attribute provides a description of the service group to the SESM. If this attribute is omitted, the service group profile name is used.

Account-Info = "I*description*"

Syntax Description

description Description of the service group.

Example

```
Account-Info = "ICompany Intranet Access"
```

Service Group

In user profiles, this attribute subscribes a user to a service group. In service group profiles, this attribute lists the service subgroups that belong to this service group.

Account-Info = "G*name*"

Syntax Description

name Name of the group profile.

Example

```
Account-Info = "GServiceGroup1"
```



Note There can be multiple instances of this attribute within a user or service group profile. Use one attribute for each service subgroup.

Service Name

In user profiles, this attribute subscribes the user to the specified service. In service group profiles, this attribute lists services that belong to the service group.

Account-Info = "Nname"

Syntax Description

name Name of the service profile.

Example

```
Account-Info = "Ncisco.com"
```



Note There can be multiple instances of this attribute within a user or service profile. Use one attribute for each service.

Example Service Group Profile

The following is an example of a service group profile. The profile is formatted for use with a freeware RADIUS server:

```
ServiceGroup1 Password = "cisco", Service-Type = outbound,
Account-Info = "Nservice1.com",
Account-Info = "Ngamers.net",
Account-Info = "GServiceGroup3",
Account-Info = "GServiceGroup4",
Account-Info = "IStandard User Services"
```

The following is the same service group profile, formatted for CiscoSecure ACS for UNIX:

```
user = ServiceGroup1 {
radius = SSG {
check_items = {
2 = "cisco"
6 = 5
}
reply_attributes = {
9,250 = "Nservice1.com"
9,250 = "Ngamers.net"
9,250 = "GServiceGroup3"
9,250 = "GServiceGroup4"
9,250 = "IStandard User Services"
}
}
}
```

Pseudo-Service Profiles

This section describes pseudo-service profiles that are used to define variable length tables or lists of information in the form of services. There are currently two types of pseudo-service profiles: Transparent Passthrough Filter and Next Hop Gateway. The following sections describe both profiles.

Transparent Passthrough Filter Pseudo-Service Profile

Transparent passthrough is designed to allow unauthenticated traffic (users or network devices that have not logged in to the SSG through the SESM) to be routed through normal IOS processing. Transparent passthrough is supported only in Cisco IOS Releases 12.0(3)DC and 12.0(5)DC.

Table 4-15 lists the Cisco AVPair attributes that appear within transparent passthrough filter pseudo-service profiles. The Cisco-AVpair attributes are used to configure ACLs.

Table 4-15 Transparent Passthrough Filter Pseudo-Service Profile Attributes

Attribute	Usage
Downstream Access Control List (outacl)	Specifies either an IOS standard access control list or an extended access control list to be applied to downstream traffic going to the user.
Upstream Access Control List (inacl)	Specifies either an IOS standard access control list or an extended access control list to be applied to upstream traffic coming from the user.

Downstream Access Control List

This attribute specifies either an IOS standard access control list or an extended access control list to be applied to downstream traffic going to the user.

Cisco-AVpair = “ip:outacl[#number]={*standard-access-control-list* | *extended-access-control-list*}”

Syntax Description

<i>number</i>	Access list identifier.
<i>standard-access-control-list</i>	Standard access control list.
<i>extended-access-control-list</i>	Extended access control list.

Example

```
Cisco-AVpair="ip:outacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21"
```



Note

There can be multiple instances of this attribute within profiles. Use one attribute for each access control list statement. Multiple attributes can be used for the same ACL. Multiple attributes are downloaded according to the number specified and executed in that order.

Upstream Access Control List

This attribute specifies either an IOS standard access control list or an extended access control list to be applied to upstream traffic coming from the user.

Cisco-AVpair = "ip:inacl[#number]={standard-access-control-list | extended-access-control-list}"

Syntax Description

<i>number</i>	Access list identifier.
<i>standard-access-control-list</i>	Standard access control list.
<i>extended-access-control-list</i>	Extended access control list.

Example

```
Cisco-AVpair="ip:inacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21"
```



Note There can be multiple instances of this attribute within profiles. Use one attribute for each access control list statement. Multiple attributes can be used for the same ACL. Multiple attributes are downloaded according to the number specified and executed in that order.

The Transparent Passthrough Filter pseudo-service profile allows or denies access to IP addresses and ports accessed through the transparent passthrough feature.

To define what traffic can pass through, the SSG downloads the Transparent Passthrough Filter pseudo-service profile. This profile contains a list of access control list (ACL) attributes. Each item contains an IP address or range of IP addresses, a list of port numbers, and specifies whether traffic is allowed or denied.

To create a filter for transparent passthrough, create a profile that contains ACL attributes that define what can and cannot be accessed.

You can also create ACLs locally. For more information, see the **ssg pass-through** command in the Cisco 6400 Command Reference.

Example Transparent Passthrough Filter Pseudo-Service Profile

The following is an example of the Transparent Passthrough Filter pseudo-service profile. The profile is formatted for use with a freeware RADIUS server:

```
ssg-filter Password = "cisco", Service-Type = outbound,
Cisco-AVpair="ip:inacl#3=deny tcp 192.168.1.0 0.0.0.255 any eq 21",
Cisco-AVpair="ip:inacl#7=permit ip any any"
```

The following is the same profile as above, formatted for CiscoSecure ACS for UNIX:

```
user = ssg-filter {
radius = SSG {
check_items = {
2 = "cisco"
6 = 5

reply_attributes = {
9,1 = "ip:inacl#3=deny tcp 192.168.1.0 0.0.0.255 any eq 21",
9,1 = "ip:inacl#7=permit ip any any"
}
}
}
```

Next Hop Gateway Pseudo-Service Profile

Because multiple SSGs might access services from different networks, each service profile can specify a next hop key, which is any string identifier, rather than an actual IP address. For each SSG to determine the IP address of the next hop, each SSG downloads its own next hop gateway table that associates keys with IP addresses.

Table 4-16 Next Hop Gateway Pseudo-Service Profile Attributes

Attribute	Usage
Next Hop Gateway Table Entry	Associates next hop gateway keys with IP addresses.

Next Hop Gateway Table Entry

Because multiple SSGs might access services from different networks, each service profile specifies a next hop key rather than an actual IP address. For each SSG to determine the IP address of the next hop, each SSG downloads its own next hop gateway table that associates keys with IP addresses. For information on defining next hop keys, see the “Service Next Hop Gateway” section.



Note

This attribute is only used in Next Hop Gateway pseudo-service profiles and should not appear in service profiles or user profiles.

Control-Info = “Gkey;ip_address”

Syntax Description

key Service name or key specified in the Service Next Hop Gateway service profile.
ip_address IP address of the next hop for this service.

Usage

Use this attribute to create a next hop gateway table for the selected SSG.

To define the IP address of the next hop for each service, the SSG downloads a special service profile that associates the next hop gateway key for each service with an IP address.

To create a next hop gateway table, create a service profile and give it any name. Use this attribute to associate service keys with their IP addresses. When you have finished, repeat this for each SSG.

For more information, see the **ssg next-hop** command in the Cisco 6400 Command Reference.

Example

```
Control-Info = "GNHT_for_SSG_1;192.168.1.128"
```

To create a next hop gateway table, create a profile and give it any name. Use the Next Hop Gateway Entry attribute to associate service keys with their IP addresses. When you have finished, repeat this for each SSG if the next hop IP addresses are different. For an example next hop gateway pseudo-service profile, see “Example Transparent Passthrough Filter Pseudo-Service Profile”.

For more information, see the **ssg next-hop** command in the Cisco 6400 Command Reference.

Example NextHop Gateway Pseudo-Service Profile

The following is an example of the Next Hop Gateway pseudo-service profile. The profile is formatted for use with a freeware RADIUS server:

```
nht1      Password = "cisco", Service-Type = outbound,
Account-Info = "Gservice3;192.168.103.3",
Account-Info = "Gservice2;192.168.103.2",
Account-Info = "Gservice1;192.168.103.1",
Account-Info = "GLabservices;192.168.4.2",
Account-Info = "GWorldwide_Gaming;192.168.4.2"
```

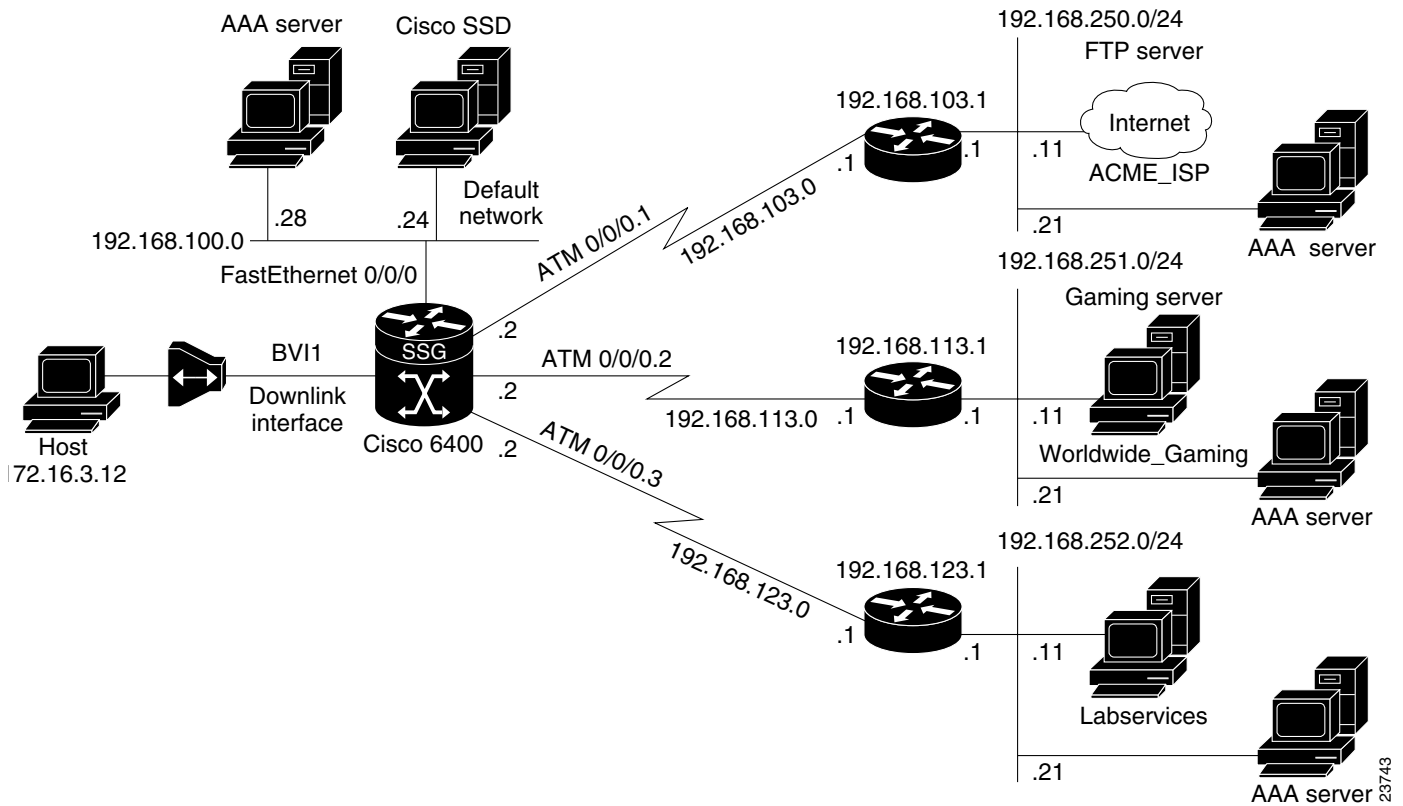
The following is the same Next Hop Gateway pseudo-service profile, formatted for CiscoSecure ACS for UNIX:

```
user = nht1{
radius= SSG {
check_items= {
2=cisco
6=5
}
reply_attributes= {
9,253="Gservice3;192.168.103.3"
9,253="Gservice2;192.168.103.2"
9,253="Gservice1;192.168.103.1"
9,253="GLabservices;192.168.4.2"
9,253="GWorldwide_Gaming;192.168.4.2"
}
}
```

Configuration Example

The configuration examples in this section support the network topology shown in Figure 4-2. These examples apply to the SSG used with SSD or SESM in RADIUS mode.

Figure 4-2 Example SSG Network Topology



Security

```

aaa new-model
aaa authentication ppp default radius
aaa authorization network default radius
ssg service-password cisco
ssg radius-helper auth-port 1645 acct-port 1646
ssg radius-helper key cisco
radius-server host 192.168.100.28 auth-port 1645 acct-port 1646
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication

```

Default Network

```

ssg default-network 192.168.100.24 255.255.255.255

```

Interfaces

```

ssg bind direction uplink ATM0/0/0.1
ssg bind direction uplink ATM0/0/0.2
ssg bind direction uplink ATM0/0/0.3
ssg bind direction downlink BVI1

```

Services

```

ssg bind service Labservices 192.168.123.1
ssg bind service Worldwide_Gaming 192.168.113.1
ssg bind service ACME_ISP 192.168.103.1
ssg next-hop download nhg1 cisco
ssg maxservice 10

```

The following is an example service profile as it would appear on the RADIUS server. It is formatted for CiscoSecure ACS for UNIX.

```

user = ACME_ISP{
profile_id = 2026
profile_cycle = 12
member = ServicesGroup
radius=6510-SSG-v1.1a {
check_items= {
2=cisco
6=5
}
reply_attributes= {
9,251="R192.168.250.0;255.255.255.0"
9,251="TX"
9,251="S192.168.250.11;1645;1646;cisco"
}
}
}

```

Service Search Order

```

ssg service-search-order local remote

```

Next-Hop Table

```

ssg next-hop download nht1 cisco

```

The following is an example next-hop table as it would appear on the RADIUS server. It is formatted for CiscoSecure ACS for UNIX.

```

ssg next-hop download nht1 cisco

user = nht1{
radius= SSG {
check_items= {
2=cisco
6=5
}
reply_attributes= {
9,253="GACME_ISP;192.168.103.1"
9,253="GLabservices;192.168.123.1"
9,253="GWorldwide_Gaming;192.168.113.1"
}
}
}

```


Max Services

```
ssg maxservice 10
```

Local Service Profile

```
local-profile Labservices
attr 26 9 251 "R192.168.123.1;255.255.255.0"
attr 26 9 251 "S192.168.252.11;1645;1646;cisco"
attr 26 9 251 "OAnyProxyService.Com"
attr 26 9 251 "TX"
attr 2 "cisco"
attr 6 5
```

Transparent Passthrough Filter

```
ssg pass-through filter download tptfilter1 cisco
```

The following is an example transparent passthrough filter as it would appear on the RADIUS server. It is formatted for CiscoSecure ACS for UNIX.

```
user = tptfilter1{
radius= SSG {
check_items= {
2=cisco
6=5
}
reply_attributes= {
9,1="ip:inacl#2=deny tcp 172.16.4.0 0.0.0.255 192.168.250.0 0.0.0.255 eq 23"
9,1="ip:inacl#5=permit ip any any"
9,1="ip:inacl#1=permit tcp any any established"
}
}
}
```

Redundancy

```
redundancy
main-cpu
auto-sync standard
no secondary console enable
```

Fastswitching

There is nothing in the running configuration for fastswitching when it is enabled.

Multicast

```
ssg multicast
```

RADIUS Interim Accounting

```
ssg accounting interval 600
```

The following example RADIUS accounting records are sent to the appropriate server every 600 seconds while the user is logged on to the SSG:

Account Update

```
NAS-IP-Address = 172.16.11.1
NAS-Port = 0
NAS-Port-Type = Virtual
User-Name = "cisco"
Acct-Status-Type = Update
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "00000000"
Acct-Session-Time = 77
Acct-Input-Octets = 0
Acct-Output-Octets = 0
Acct-Input-Packets = 0
Acct-Output-Packets = 0
Framed-Protocol = PPP
Framed-IP-Address = 172.16.11.12
Control-Info = "I0;0"
Control-Info = "O0;0"
Acct-Delay-Time = 0
```

Connection Update

```
NAS-IP-Address = 172.16.11.1
NAS-Port = 0
NAS-Port-Type = Virtual
User-Name = "cisco"
Acct-Status-Type = Update
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "00000012"
Acct-Session-Time = 8
Acct-Input-Octets = 0
Acct-Output-Octets = 0
Acct-Input-Packets = 0
Acct-Output-Packets = 0
Framed-Protocol = PPP
Control-Info = "I0;0"
Control-Info = "O0;0"
Service-Info = "Nservice.com"
Service-Info = "Uname"
Service-Info = "TX"
Acct-Delay-Time = 0
```

CEF

```
ip cef
```

IOS NAT

```
interface ATM0/0/0.10 multipoint
 ip address 192.168.103.12 255.255.255.0
```

```

no ip directed-broadcast
ip nat outside
ip pim sparse-dense-mode
ip pim multipoint-signalling
map-group mapgroup1
atm multipoint-signalling
atm esi-address 2020202020.10

interface Virtual-Template1
ip unnumbered FastEthernet0/0/0
no ip directed-broadcast
ip nat inside
ip mroute-cache
keepalive 60
peer default ip address pool pool1
ppp authentication pap

```

Service Name to VC Mapping

```
ssg vc-service-map public1 1/37 non-exclusive
```

Monitoring and Troubleshooting SSG

Table 4-17 describes the commands that help you monitor and maintain the SSG.

Table 4-17 SSG Monitoring and Troubleshooting Commands

Command	Purpose
Router# show ssg connection <i>ip-address service-name</i>	Displays the connections of a given host and service name.
Router# clear ssg connection <i>ip-address service-name</i>	Removes the connections of a given host and service name.
Router# show ssg pass-through-filter	Displays the downloaded filter for transparent passthrough.
Router# clear ssg pass-through-filter	Removes the downloaded filter for transparent passthrough. To remove the filter from NVRAM, enter the no form of the ssg pass-through command.
Router# show ssg host [<i>ip-address</i>] [<i>username</i>]	Displays the information about a subscriber and the current connections of the subscriber.
Router# clear ssg host <i>ip-address</i>	Removes a given host or subscriber.
Router# show ssg direction	Displays the direction of all interfaces for which a direction has been specified.
Router# show ssg next-hop	Displays the next-hop table.
Router# clear ssg next-hop	Removes the next-hop table. To remove the next-hop table from NVRAM, enter the no form of the ssg next-hop command. (See the Cisco 6400 Command Reference.)
Router# show ssg binding	Displays service names that have been bound to interfaces and the interfaces to which they have been bound.
Router# show ssg service <i>service-name</i>	Displays the information for a service.
Router# clear ssg service <i>service-name</i>	Removes a service.

RADIUS

To troubleshoot communication between the RADIUS server and the NRP, enter the **debug radius** command.



Point-to-Point Protocol

This chapter describes the Point-to-Point Protocol features supported in Cisco IOS Release 12.2(2)B.

Restrictions

PPPoE

- Point-to-point protocol over Ethernet (PPPoE) is supported on ATM permanent virtual circuits (PVCs) only.
- The Cisco 6400 can not initiate dial-out PPPoE sessions.
- PPPoE supports Cisco Express Forwarding (CEF) only. Fastswitching on PPPoE virtual-access interfaces is not supported.

PPPoA

- The PPP Autosense feature only supports point-to-point protocol over ATM (PPPoA) sessions that are Logical Link Control (LLC) encapsulated.
- Do not use this feature on a router that initiates PPPoA sessions.
- PPPoA does not support static IP assignments within virtual templates.

PPPoE Session Count MIB

- Using the **snmp-server enable traps pppoe** command enables SNMP traps only and does not support inform requests.

Prerequisites

The Cisco 6400 node route processor (NRP) requires 128MB of DRAM to support up to 2800 concurrent PPPoE sessions. An NRP with 64MB DRAM can support up to 2000 concurrent PPPoE sessions.

Configuration Tasks

This section contains the following tasks:

- Configuring PPPoA
- Configuring PPPoE

- Configuring PPP Autosense
- Configuring AAA Authentication
- Configuring PPPoE Session Limit
- Configuring PPPoE Session Count MIB

Configuring PPPoA

Before configuring this feature see the restrictions for PPPoA.

The following tasks provide the minimum steps needed to configure PPP over ATM on the Cisco 6400 NRP. For more information about PPP over ATM, see “Configuring ATM” in the Wide-Area Networking Configuration Guide of the Cisco IOS 12.1 documentation set.

Configuring a PPP Virtual Template

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 all 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.

To configure a virtual template, perform these steps starting in global configuration mode:

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

Examples

The following example shows a typical virtual template configuration for the Cisco 6400 NRP:

```
Router(config)# interface virtual-template 1
Router(config-if)# ip unnumbered fastethernet 0/0/0
```

```

router(config-if)# peer default ip address pool telecommuters
Router(config-if)# ppp authentication chap
Router(config-if)# exit
Router(config)# ip local pool telecommuters 10.36.1.1 10.36.1.254

```

In this configuration, it is assumed that all PPP over ATM 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 PPP over ATM connection is running without an IP address (recommended). Instead, the IP address of the FastEthernet interface is used for addressability.

To configure a different class of users on the same router, you can provision a separate virtual template interface. The following shows a DHCP server rather than a local pool and PAP authentication over CHAP:

```

Router(config)# interface Virtual-Template 2
Router(config-if)# ip unnumbered fastethernet 0/0/0
Router(config-if)# peer default ip address dhcp
Router(config-if)# ppp authentication pap chap
Router(config-if)# exit
Router(config)# ip dhcp-server 10.5.20.149

```

Up to 25 virtual templates can be configured.

Configuring AAA Authentication

A AAA authentication database, such as RADIUS or TACACS+, can be used to configure the user’s virtual access interface. To configure AAA authentication for PPP over ATM, see “Configuring AAA Authentication” for configuration tasks.

Configuring PVCs

After you have configured a virtual template for PPP over ATM, you must configure the PVCs that carry traffic from the NRP to the ATM interfaces. To configure PPP over ATM on a PVC, enter the following commands starting in global configuration mode:

	Command	Purpose
Step 1	<code>interface atm 0/0/0 [.subinterface-number {multipoint point-to-point}]</code>	Specifies the ATM interface and optional subinterface.
Step 2	<code>pvc [name] vpi/vci</code>	Configures a new ATM PVC by assigning a name (optional) and VPI/VCI numbers.
Step 3	<code>encapsulation aal5mux ppp virtual-Template number</code>	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, as shown in the *Cisco 6400 Software Configuration Guide and Command Reference*, “Configuring the NRP” chapter, “Working with Permanent Virtual Circuits” section.

Example

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

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

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

Router(config)# interface atm 0/0/0.40 multipoint
Router(config-subif)# pvc 0/50
Router(config-if-atm-vc)# encapsulation aal5mux ppp virtual-template 1
Router(config-if-atm-vc)# exit
Router(config-subif)# pvc 0/51
Router(config-if-atm-vc)# encapsulation aal5mux ppp virtual-template 1
Router(config-if-atm-vc)# exit
```

Verifying and Troubleshooting PPPoA

The global configuration command **show atm pvc ppp** shows the PPP over ATM 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 PPP over ATM session. A subsequent **show interface virtual-access** command gives 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 this 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.

Configuring PPPoE

Before configuring this feature see the restrictions for PPPoE and the Prerequisites section.

Perform the following tasks to configure PPP over Ethernet on ATM:

- Configuring a Virtual Template for PPPoE
- Configuring PPPoE on an ATM Interface
- Setting the IP MTU

Configuring a Virtual Template for PPPoE

To configure PPPoE on a virtual-access interface, enter the following commands starting in global configuration mode.

	Command	Purpose
Step 1	<code>Router(config)#vpdn enable</code>	Enables virtual private dial-up networking.
Step 2	<code>Router(config)#vpdn-group number</code>	Selects VPDN-group configuration mode.
Step 3	<code>Router(config-vpdn)#accept dialin pppoe virtual-template number</code>	Configures the router to accept dial-in PPPoE calls.
Step 4	<code>Router(config-vpdn)#pppoe limit per-mac number</code>	(Optional) Limits the number of PPPoE sessions that originate from one MAC address. Default is 100.
Step 5	<code>Router(config-vpdn)#pppoe limit per-vc number</code>	(Optional) Limits the number of PPPoE sessions that can be established on a virtual circuit. Default is 100.
Step 6	<code>Router(config-vpdn)#exit</code>	Returns to global configuration mode.
Step 7	<code>Router(config)#virtual-template template-number pre-clone number</code>	(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, a number of pre-cloned virtual-access interfaces may be created and saved to a private PPPoE list. This cloning procedure reduces the CPU workload while PPPoE sessions are established.

Configuring PPPoE on an ATM Interface

To configure PPPoE on an ATM interface, enter the following commands starting in global configuration mode.

	Command	Purpose
Step 1	<code>Router(config)#interface atm slot/0.subinterface-number multipoint</code>	Specifies an ATM multipoint subinterface.
Step 2	<code>Router(config-if)#pvc [name] VPI/VCI</code>	Configures the PVC.
Step 3	<code>Router(config-if)#encapsulation aal5snap</code>	Configures SNAP encapsulation.
Step 4	<code>Router(config-if)#protocol pppoe</code>	Selects PPPoE as the protocol for the PVC.
Step 5	<code>Router(config)#exit</code>	Returns to global configuration mode.

Setting the IP MTU

To allow PPPoE to operate over the virtual-access interface, the IP maximum transmission unit (MTU) must be set to 1492. Enter the following commands, starting in global configuration mode, to set the IP MTU.

	Command	Purpose
Step 1	<code>Router(config)#interface virtual-template number</code>	Selects the virtual-access interface to be configured.
Step 2	<code>Router(config-if)#ip mtu 1492</code>	Sets the IP MTU to 1492.
Step 3	<code>Router(config)#exit</code>	Returns to global configuration mode.

Verifying PPPoE

- Step 1** Enter the **show vpdn** command from interface configuration mode. This output shows PPPoE session information. 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
```

The session information fields from the **show vpdn** display are detailed below:

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** command from interface configuration mode. 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.
```

Example: PPPoE

This section provides the following configuration examples:

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

PPPoE Configuration on a PVC

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

```
Router(config)#vpdn enable
Router(config)#vpdn-group 1
Router(config-vpdn)#accept dialin pppoe virtual-template 1
Router(config-vpdn)#exit
Router(config)#virtual-template 1 pre-clone 500

Router(config)#interface atm 2/0.1 multipoint
Router(config-if)#pvc 0/60
Router(config-if-atm-vc)#encapsulation aal5snap
Router(config-if-atm-vc)#protocol pppoe
Router(config-if-atm-vc)#exit
```

```

Router(config-if)#exit

Router(config)#ip cef
Router(config)#interface virtual-template 1
Router(config-if)#ip address 10.0.1.2 255.255.255.0
Router(config-if)#ip mtu 1492
Router(config-if)#ip route-cache cef
Router(config-if)#exit

```

PPPoE Configuration Using 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:

```

Router(config)#vppdn enable
Router(config)#vppdn-group 1
Router(config-vppdn)#accept dialin pppoe virtual-template 1
Router(config-vppdn)#exit
Router(config)#virtual-template 1 pre-clone 500

Router(config)#interface atm 2/0.1 multipoint
Router(config-if)#pvc 0/60
Router(config-if-atm-vc)#class users
Router(config-if-atm-vc)#exit
Router(config-if)#exit

Router(config)#vc-class atm users
Router(vc-class)#encapsulation aal5snap
Router(vc-class)#protocol pppoe
Router(vc-class)#exit

Router(config)#ip cef
Router(config)#interface virtual-template 1
Router(config-if)#ip address 10.0.1.2 255.255.255.0
Router(config-if)#ip mtu 1492
Router(config-if)#ip route-cache cef
Router(config-if)#exit

```

Concurrent PPPoE and Bridging

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

```

Router(config)#vppdn enable
Router(config)#vppdn-group 1
Router(config-vppdn)#accept dialin pppoe virtual-template 1
Router(config-vppdn)#exit
Router(config)#virtual-template 1 pre-clone 500
Router(config)#bridge 1 protocol ieee
Router(config)#bridge 1 route ip

Router(config)#interface atm 2/0.1 multipoint
Router(config-if)#bridge-group 1
Router(config-if)#pvc 0/60
Router(config-if-atm-vc)#encapsulation aal5snap
Router(config-if-atm-vc)#protocol pppoe
Router(config-if-atm-vc)#exit
Router(config-if)#exit

Router(config)#ip cef
Router(config)#interface virtual-template 1
Router(config-if)#ip address 10.0.1.2 255.255.255.0
Router(config-if)#ip mtu 1492

```

```
Router(config-if)#ip route-cache cef
Router(config-if)#exit
```

Monitoring and Maintaining PPPoE

Table 5-1 describes the commands that help you monitor and maintain PPOE.

Table 5-1 PPPoE Monitoring and Maintaining Commands

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.

Troubleshooting Tips

Concurrent Bridging and PPPoE

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.

VC Classes

You can also configure PPP over Ethernet in a VC class and apply this VC class to an ATM VC, subinterface, or interface. For information about configuring a VC class, refer to the section "Configure VC Classes" in the chapter "Configuring ATM" of the *Wide-Area Networking Configuration Guide for Cisco IOS Release 12.1*.

Cisco Express Forwarding

In order to gain maximum packet switching performance, Cisco Express Forwarding (CEF) should be enabled on the virtual-access interface. For information about enabling Cisco Express Forwarding, refer to the section "Configuring Cisco Express Forwarding" in the chapter "Cisco Express Forwarding" of the *Cisco IOS Switching Services Configuration Guide for IOS Release 12.1*.

Configuring PPP Autosense

PPP Autosense can be configured on a single PVC, or on a VC class that can be applied to all PVCs on an ATM interface.

To configure PPP Autosense on a 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)# pvc [name] vpi/vci	Configures a PVC on the ATM interface or subinterface.
Step 3	Router(config-if-atm-vc)# encapsulation aal5autopp Virtual-Template number	Configures PPP Autosense on the PVC. Also specifies the virtual template interface to use to clone the new virtual access interfaces for PPPoA sessions on this PVC.

To configure PPP Autosense on a 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 aal5autopp Virtual-Template number	Configures PPP 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.

**Note**

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

Verifying PPP Autosense Configuration

To verify that you successfully configured PPP Autosense, enter the **show running-config EXEC** command.

Example: PPP Autosense

This section provides the following configuration examples:

- PPP Autosense on a PVC
- PPP Autosense on a VC Class
- PPP Autosense on Multiple VC Classes and Virtual Templates

PPP Autosense on a PVC

In the following example, the NAS is configured with PPP Autosense on PVC 30/33.

```

!
! Configure PPP Autosense
!
interface ATM 0/0/0.33 multipoint
  pvc 30/33
    encapsulation aal5autopp 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
  ip mtu 1492
  ip route-cache cef
!
! Enable precloning for virtual-template 1
!
virtual-template 1 pre-clone 2000
!

```

PPP Autosense on a VC Class

In the following example, the NAS is configured with PPP Autosense on the VC class called “MyClass.” MyClass applies the PPP Autosense feature to all PVCs on the ATM 0/0/0.99 interface.

```

!
! Configure PPP Autosense
!
vc-class ATM MyClass
  encapsulation aal5autopp 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
  ip mtu 1492
  ip route-cache cef
!
! Enable precloning for virtual-template 1
!
virtual-template 1 pre-clone 2000
!

```

PPP 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 aal5autopp Virtual-Template1
!
vc-class atm pppoa
  encapsulation aal5autopp Virtual-Template2
!

```


Monitoring and Maintaining PPP Autosense

Table 5-2 describes the commands that help you monitor and maintain PPOA.

Table 5-2 PPPoA Monitoring and Maintaining Commands

Command	Purpose
Router# <code>show atm pvc ppp</code>	After the client at the other end of the PPP Autosense PVC initiates a PPPoA session, enter this command to check that the PVC contains the PPPoA session.
Router# <code>show caller</code>	Enter this command to: <ul style="list-style-type: none"> • 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 that 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# <code>show interface virtual access number</code>	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 Tips

To troubleshoot PPP sessions establishment, enter 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, enter the following commands:

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



Note

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

Configuring AAA 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 chapter “Authentication, Authorization, and Accounting (AAA)” in the *Cisco IOS Security Configuration Guide*.

To configure the router to use AAA for PPP authentication only, enter the following configuration commands:

	Command	Description
Step 1	<code>aaa new-model</code>	Enables the AAA access control model.
Step 2	<code>aaa authentication ppp {default list-name} method1 [method2...]</code>	Specifies one or more AAA 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), and the *method* option is a list of methods. For example, to configure virtual template 3 to use TACACS+ before RADIUS, and virtual template 4 to use RADIUS before local authentication, enter the following configuration commands:

```
Router(config)# aaa new-model
Router(config)# aaa authentication ppp list1 tacacs+ radius
Router(config)# aaa authentication ppp list2 radius local

Router(config)# interface virtual-template 3
Router(config-if)# ip unnumbered fastethernet 0/0/0
Router(config-if)# ppp authentication chap list1
Router(config-if)# exit

Router(config)# interface virtual-template 4
Router(config-if)# ip unnumbered fastethernet 0/0/0
Router(config-if)# ppp authentication chap list2
Router(config-if)# ^z
```

Using a Local Authentication Database

Enter the `aaa authentication ppp` command with the method keyword **local** to specify that the Cisco router or access server will use the local username database for authentication. The following example shows how to configure authentication by using the local username database:

```
Router(config)# aaa new-model
Router(config)# aaa authentication ppp default local
```

Configuring a RADIUS Server

To configure the NRP to use a RADIUS server, enter the following commands starting in global configuration mode:

	Command	Purpose
Step 1	<code>radius-server host {hostname ip-address} [auth-port port-number] [acct-port port-number]</code>	Specifies a RADIUS server host.
Step 2	<code>radius-server key key</code>	Sets the encryption key to match that used on the RADIUS server.
Step 3	<code>radius-server attribute nas-port format d</code>	Selects the ATM VC extended format (d) for the NAS port field.

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

```
Router(config)# aaa new-model
Router(config)# aaa authentication ppp default radius

Router(config)# radius-server host 172.31.5.96 auth-port 1645 acct-port 1646
Router(config)# radius-server key foo
Router(config)# radius-server attribute nas-port format d
```

The authentication and accounting port need not be specified, because they default to 1645 and 1646, respectively.

Configuring a TACACS+ Server

To configure the NRP to use a TACACS+ server, enter the following commands starting in global configuration mode:

	Command	Purpose
Step 1	<code>tacacs-server host {hostname ip-address} [single-connection] [port integer] [timeout integer] [key string]</code>	Specifies a TACACS+ server host.
Step 2	<code>tacacs-server key key</code>	Sets the encryption key to match that used on the TACACS+ daemon.

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

```
Router(config)# aaa new-model
Router(config)# aaa authentication ppp default tacacs+

Router(config)# tacacs-server host 172.31.5.96
Router(config)# tacacs-server key foo
```

Configuring PPPoE Session Limit

Overview

The PPPoE Session Limit feature enables you to limit the number of PPP over Ethernet (PPPoE) sessions that can be created on a router or on an ATM permanent virtual circuit (PVC), PVC range, or virtual circuit (VC) class.

Before the introduction of this feature, there was no way to limit the number of PPPoE sessions that could be created on a router. Not having a limit was potentially a problem because it was possible that the router could create so many PPPoE sessions that it would run out of memory.

To prevent the router from using too much memory for virtual access, the PPPoE Session Limit feature introduces a new command and a modification to an existing command that enable you to specify the maximum number of PPPoE sessions that can be created. Using the new **pppoe limit max-sessions** command limits the number of PPPoE sessions that can be created on the router. Using the modified **pppoe max-sessions** command limits the number of PPPoE sessions that can be created on an ATM PVC, PVC range, VC class, or Ethernet subinterface.

PPPoE Session Limit Types

There are three basic types of limits that can be applied to PPPoE sessions. These session limit types work independently of each other. The following statements describe these limits:

- PPPoE session limits on the router.

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

- PPPoE session limits based on a MAC address.

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

- PPPoE session limits on a physical port.

This type of limit applies to PVCs or VLANs and can be applied globally or to specific PVCs or VLANs.

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

Benefits

The PPPoE Session Limit feature prevents the router from using too much memory for virtual access by enabling you to limit the number of PPPoE sessions that can be created on a router or on an PVC, ATM PVC range, or VC class.

Configuration Tasks

To configure PPPoE sessions limits, complete one or more of the following tasks:

- Limiting the Number of PPPoE Sessions on the Router (optional)
- Limiting the Number of PPPoE Sessions on a PVC (optional)
- Limiting the Number of PPPoE Sessions in a VC Class (optional)
- Limiting the Number of PPPoE Sessions in an ATM PVC Range (optional)
- Limiting the Number of PPPoE Sessions on an Individual PVC Within a PVC Range (optional)

To verify PPPoE sessions limits, complete the following task:

- Verifying PPPoE Session Limits (optional)

Limiting the Number of PPPoE Sessions on the Router

To specify the maximum number of PPPoE sessions that can be created on a router, use the following command in VPDN group configuration mode:

Command	Purpose
Router(config-vpdn)# pppoe limit max-sessions number-of-sessions	Specifies the maximum number of PPPoE sessions that are permitted on the router.

PPPoE session limits configured by using the **pppoe limit max-session** command take precedence over limits configured using the **pppoe limit per-vlan** and **pppoe limit per-mac** commands.

Limiting the Number of PPPoE Sessions on a PVC

To specify the maximum number of PPPoE sessions that can be created on a PVC, use the following command in interface-ATM-VC configuration mode:

Command	Purpose
Router(config-if-atm-vc)# pppoe max-sessions <i>number-of-sessions</i>	Specifies the maximum number of PPPoE sessions that are permitted on the PVC.

PPPoE session limits created on a PVC by using the **pppoe max-sessions** command take precedence over the limits created with the **pppoe limit per-vc** command.

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

Limiting the Number of PPPoE Sessions in a VC Class

To specify the maximum number of PPPoE sessions that can be created in a VC class, use the following command in VC-class configuration mode:

Command	Purpose
Router(config-vc-class)# pppoe max-sessions <i>number-of-sessions</i>	Specifies the maximum number of PPPoE sessions that are permitted in the VC class.

PPPoE session limits created in a VC class by using the **pppoe max-sessions** command take precedence over the limits created with the **pppoe limit per-vc** command.

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

Limiting the Number of PPPoE Sessions in an ATM PVC Range

To specify the maximum number of PPPoE sessions that can be created in an ATM PVC range, use the following command in ATM PVC range configuration mode:

Command	Purpose
Router(config-if-atm-range)# pppoe max-sessions <i>number-of-sessions</i>	Specifies the maximum number of PPPoE sessions that are permitted in the range.

PPPoE session limits created in an ATM PVC range by using the **pppoe max-sessions** command take precedence over the limits created with the **pppoe limit per-vc** command.

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

Limiting the Number of PPPoE Sessions on an Individual PVC Within a PVC Range

To specify the maximum number of PPPoE sessions that can be created on an individual PVC within a PVC range, use the following command in ATM PVC-in-range configuration mode:

Command	Purpose
Router(cfg-if-atm-range-pvc)# pppoe max-sessions <i>number-of-sessions</i>	Specifies the maximum number of PPPoE sessions that are permitted on the PVC.

PPPoE session limits created on an individual PVC within a range by using the **pppoe max-sessions** command take precedence over the limits created with the **pppoe limit per-vc** command.

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

Verifying PPPoE Session Limits

To verify that PPPoE session limits are configured correctly, use the following command in privileged EXEC mode:

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

Monitoring and Maintaining PPPoE Session Limits

To monitor PPPoE sessions limits, use the following command in EXEC mode:

Command	Purpose
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.

Configuration Examples

This section provides the following configuration examples:

- Limiting the Number of PPPoE Sessions on the Router Example
- Limiting the Number of PPPoE Sessions on an ATM PVC Example
- Limiting the Number of PPPoE Sessions in an ATM VC Class Example
- Limiting the Number of PPPoE Sessions in an ATM PVC Range Example
- Limiting the Number of PPPoE Sessions on an Individual PVC Within a PVC Range Example

Limiting the Number of PPPoE Sessions on the Router Example

The following example shows a limit of 100 PPPoE sessions configured for the router:

```
vpdn enable

vpdn-group 1
 accept dialin
  protocol pppoe
  virtual-template 1
 pppoe limit max-sessions 100
```

Limiting the Number of PPPoE Sessions on an ATM PVC Example

The following example shows a limit of 10 PPPoE sessions configured for the PVC:

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

Limiting the Number of PPPoE Sessions in an ATM VC Class Example

The following example shows a limit of 20 PPPoE sessions configured for the VC class called “main”:

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

Limiting the Number of PPPoE Sessions in an ATM PVC Range Example

The following example shows a limit of 30 PPPoE sessions configured for the ATM PVC range called “range-1”:

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

Limiting the Number of PPPoE Sessions on an Individual PVC Within a PVC Range Example

The following example shows a limit of 10 PPPoE sessions configured for “pvc1”, which is part of the ATM PVC range called “range1”:

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

Configuring PPPoE Session Count MIB



Note

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

Overview

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 on permanent virtual circuits (PVCs) and on the router.

This new 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. The PPPoE session count thresholds can be configured by using the **pppoe limit max-sessions** and **pppoe max-sessions** commands.

Table 5-3 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 5-3 PPPoE Session Count MIB Objects and Tables.

Object	Description
cPppoeSystemCurrSessions	Number of active PPPoE sessions 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 exceeds the configured threshold value.
cPppoeVcSessionThresholdTrap	Generates a notification message when the number of PPPoE sessions on the PVC exceeds the configured threshold value.

Benefits

The PPPoE Session Count MIB provides the following benefits:

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

Configuration Tasks

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 exceeded, use the following command in global configuration mode:

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

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

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)# <code>interface atm number [point-to-point multipoint]</code>	Configures an ATM interface. To determine the correct form of the <code>interface atm</code> command, refer to your ATM network module, port adapter, or router documentation.

	Command	Purpose
Step 2	Router(config-if)# pvc [name] vpi/vci	Configures the PVC.
Step 3	Router(config-if-atm-vc)# pppoe max-session <i>number-of-sessions</i> [threshold-sessions <i>number-of-sessions</i>]	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.

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 <i>number-of-sessions</i> [threshold-sessions <i>number-of-sessions</i>]	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.

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 <i>start-vpi/start-vci end-vpi/end-vci</i>	Defines a range of ATM PVCs.
Step 3	Router(cfg-if-atm-range)# pppoe max-session <i>number-of-sessions</i> [threshold-sessions <i>number-of-sessions</i>]	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session count threshold at which an SNMP trap will be generated.

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

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 <i>start-vpi/start-vci end-vpi/end-vci</i>	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 <i>number-of-sessions</i> [threshold-sessions <i>number-of-sessions</i>]	Sets the maximum number of PPPoE sessions that will be permitted on an ATM PVC, PVC range, VC class, or VLAN, and sets the PPPoE session count threshold at which an SNMP trap will be generated.

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

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 Level 2 Forwarding (L2F) Protocol tunnel and message identifiers in a VPDN.

Configuration Examples

This section provides the following configuration examples:

- Configuring PPPoE Session Count SNMP Traps Example
- PPPoE Session Count Threshold for the Router Example
- PPPoE Session Count Threshold for a PVC Example
- PPPoE Session Count Threshold for a VC Class Example
- PPPoE Session Count Threshold for a PVC Range Example
- PPPoE Session Count Threshold for an Individual PVC Within a PVC Range Example

Configuring PPPoE Session Count SNMP Traps Example

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
```

PPPoE Session Count Threshold for the Router Example

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 exceeds 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
```

PPPoE Session Count Threshold for a PVC Example

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 exceeds 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
```

PPPoE Session Count Threshold for a VC Class Example

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 exceeds 3, an SNMP trap is generated.

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

PPPoE Session Count Threshold for a PVC Range Example

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

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

PPPoE Session Count Threshold for an Individual PVC Within a PVC Range Example

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 exceeds 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
```




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(2)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, page 6-1
- Restrictions, page 6-2
- Input and Output Hold-Queues, page 6-2
- LCP Session Initiations, page 6-3
- PPP Timeouts, page 6-4
- Keepalives, page 6-5
- Virtual Access Interface Precloning, page 6-7
- L2TP Control Channel Parameters, page 6-8
- L2TP Tunnel Timeout, page 6-10
- An Example Configuration of Session and Tunnel Scalability Parameters, page 6-10
- Monitoring and Troubleshooting PPP Scalability, page 6-11
- Monitoring and Troubleshooting L2TP Scalability, page 6-12

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 6-1).

Table 6-1 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 the **show interfaces EXEC** command reveals an excessive number of discarded packets due to input or output hold-queue overflows, 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 6-1 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)# <code>lcp max-session-starts number</code>	Specifies the maximum number of simultaneous LCP sessions to be negotiated. Value must be between 100 and 3000 sessions.
Router(config)# <code>lcp max-load-metric number</code>	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 <i>number</i>	Selects or creates the virtual template interface and enters interface configuration mode.
Step 2	Router(config-if)# ppp timeout authentication <i>seconds</i>	0 - 255. Specifies the PPP authentication timeout, in seconds. Default is 10 seconds.
Step 3	Router(config-if)# ppp timeout retry <i>seconds</i>	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 <i>number</i>	Selects or creates the virtual template interface and enters interface configuration mode.
Step 2	Router(config-if)# keepalive [<i>seconds</i>]	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 <i>number</i>	Selects the VPDN group.
Step 2	Router(config-vpdn)# l2tp tunnel hello <i>hello-interval</i>	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 <i>template-number</i> pre-clone <i>number</i>	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 <i>number</i>	Selects the VPDN group.
Step 2	Router(config-vpdn)# l2tp tunnel retransmit retries <i>value</i>	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 queue size 0, max 0
Resend queue size 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	<code>Router(config)# vpdn-group number</code>	Selects the VPDN group.
Step 2	<code>Router(config-vpdn)# l2tp tunnel nosession-timeout seconds</code>	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 Troubleshooting PPP Scalability

Use the following commands to monitor and maintain 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 /
ATM Int.  Name      VPI  VCI  Type  VA  VASt  SC  Peak  Avg/Min  Burst
          Name                                Kbps  Kbps   Cells VCSt
0/0/0.101  2          1    41  PVC   1  DOWN  UBR  599040
0/0/0.101  3          1    42  PVC   2  DOWN  UBR  599040

```

```

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 Troubleshooting L2TP Scalability

For general information on monitoring and troubleshooting 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 6-2.

```
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 6-2 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.



Miscellaneous Features

This chapter describes the following features:

- Routing and Bridging, page 7-1
- ATM Routed Bridge Encapsulation, page 7-3
- RADIUS VC Logging, page 7-6
- IPCP Subnet Mask Support, page 7-9
- IP Overlapping Address Pools, page 7-13
- ATM SNMP Trap and OAM Enhancements, page 7-15

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. See the “ATM Routed Bridge Encapsulation” section on page 7-3 for routed bridging configuration tasks.

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

	Command	Purpose
Step 1	<code>interface atm 0/0/0 [.subinterface-number {multipoint point-to-point}]</code>	Specifies the ATM interface and optional subinterface.
Step 2	<code>pvc [name] vpi/vci</code>	Configures a new ATM PVC by assigning a name (optional) and VPI/VCI numbers.

	Command	Purpose
Step 3	<code>encapsulation aal5snap¹</code>	Configures AAL5 with SNAP encapsulation.
Step 4	<code>protocol protocol [protocol-address inarp] [[no] broadcast]</code>	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.

Examples

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
```

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
```

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

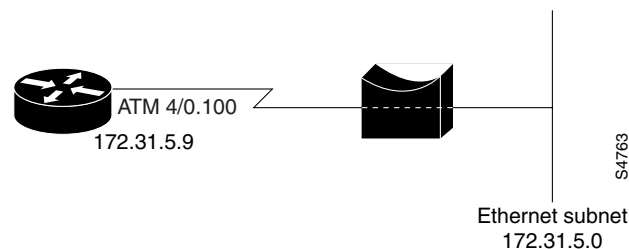
Router(config-if)# pvc 4 34
Router(config-if-atm-vc)# encapsulation aal5snap
Router(config-if-atm-vc)# protocol ip inarp broadcast
Router(config-if-atm-vc)# exit
Router(config-if)# exit

```

ATM Routed Bridge Encapsulation

The ATM routed bridge encapsulation feature on the Cisco 6400 node route processor (NRP) is used to route IP over bridged RFC 1483 Ethernet traffic from a stub-bridged LAN.

Figure 7-1 ATM Routed Bridge Encapsulation



Bridged IP packets received on an ATM interface configured in route-bridged mode are routed through the IP header. Such interfaces take advantage of the characteristics of a stub LAN topology commonly used for digital subscriber line (DSL) access and offer increased performance and flexibility over integrated routing and bridging (IRB).

Benefits

ATM routed bridge encapsulation reduces the security risk associated with normal bridging or IRB by reducing the size of the non-secured network. By using a single virtual circuit (VC) allocated to a subnet (which could be as small as a single IP address), ATM routed bridge encapsulation limits the “trust environment” to a single customer premises using IP addresses in the subnet.

Restrictions

ATM routed bridge encapsulation does not support MAC-layer access lists. Only IP access lists are supported.

Configuration Tasks

Perform the following tasks to configure ATM routed bridge encapsulation. The first task is required; the remaining tasks are optional.

- Configuring ATM Routed Bridge Encapsulation
- Verifying ATM Routed Bridge Encapsulation

Configuring ATM Routed Bridge Encapsulation

Perform the following tasks to configure ATM routed bridge encapsulation on your Cisco 6400 NRP:

	Command	Purpose
Step 1	Router(config)# interface atm <i>slot/0.subinterface-number</i> point-to-point	Specifies an ATM point-to-point interface.
Step 2	Router(config-if)# pvc <i>VPI/VCI</i>	Configures a VC to carry the routed bridge traffic.
Step 3	Router(config-if)# atm route-bridge ip	Enables ATM routed bridge encapsulation for IP.
Step 4	Router(config-if)# ip address <i>ip-address mask</i> [secondary]	Provides an IP address on the same subnetwork as the remote network.
Step 5	Router(config-if)# ^Z	Exits to EXEC mode.

Only the specified network layer (IP) will be routed. Any remaining protocols can be passed on to bridging or other protocols. In this manner, ATM routed bridge encapsulation can be used to route IP while other protocols (such as IPX) are bridged normally.

Configuration Examples

This section provides the following configuration examples:

- ATM Routed Bridge Encapsulation Example
- ATM Routed Bridge Encapsulation on an Unnumbered Interface Example
- Concurrent Bridging and ATM Routed Bridge Encapsulation Example

ATM Routed Bridge Encapsulation Example

The following example shows a typical ATM routed bridge encapsulation configuration:

```
interface atm 4/0.100 point-to-point
 ip address 172.69.5.9 255.255.255.0
 pvc 0/32
 atm route-bridged ip
```


ATM Routed Bridge Encapsulation on an Unnumbered Interface Example

The following ATM routed bridge encapsulation example uses a static route to point to an unnumbered interface:

```
interface atm 4/0.100 point-to-point
  ip unnumbered ethernet 1/0
  pvc 0/32
  atm route-bridged ip

ip route 172.69.5.9 255.255.255.0 interface atm 4/0.100
```

Concurrent Bridging and ATM Routed Bridge Encapsulation Example

The following example shows concurrent use of ATM routed bridge encapsulation with normal bridging. IP datagrams are route-bridged, while other protocols (such as IPX or AppleTalk) are bridged.

```
bridge 1 protocol ieee

interface atm 4/0.100 point-to-point
  ip address 172.69.5.9 255.255.255.0
  pvc 0/32
  bridge-group 1
  atm route-bridged ip
```

Verifying ATM Routed Bridge Encapsulation

Enter the **show ip cache** command to confirm that ATM routed bridge encapsulation is enabled:

```
Router# show ip cache
IP routing cache version 4490, 141 entries, 20772 bytes, 0 hash overflows
Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
  quiet interval 3 seconds, threshold 0 requests
Invalidation rate 0 in last 7 seconds, 0 in last 3 seconds
Last full cache invalidation occurred 0:06:31 ago
Prefix/Length      Age      Interface      MAC Header
131.108.1.1/32     0:01:09  Ethernet0/0    AA000400013400000C0357430800
131.108.1.7/32     0:04:32  Ethernet0/0    00000C01281200000C0357430800
131.108.1.12/32    0:02:53  Ethernet0/0    00000C029FD000000C0357430800
131.108.2.13/32    0:06:22  Fddi2/0        00000C05A3E000000C035753AAAA0300
                   00000800
131.108.2.160/32   0:06:12  Fddi2/0        00000C05A3E000000C035753AAAA0300
                   00000800
131.108.3.0/24     0:00:21  Ethernet1/2    00000C026BC600000C03574D0800
131.108.4.0/24     0:02:00  Ethernet1/2    00000C026BC600000C03574D0800
131.108.5.0/24     0:00:00  Ethernet1/2    00000C04520800000C03574D0800
131.108.10.15/32   0:05:17  Ethernet0/2    00000C025FF500000C0357450800
131.108.11.7/32    0:04:08  Ethernet1/2    00000C010E3A00000C03574D0800
131.108.11.12/32   0:05:10  Ethernet0/0    00000C01281200000C0357430800
131.108.11.57/32   0:06:29  Ethernet0/0    00000C01281200000C0357430800
```

Routed Bridge Encapsulation for Cisco Express Forwarding

The ATM RBE feature routes IP over bridged RFC 1483 Ethernet traffic from a stub-bridged LAN.

RADIUS VC Logging

RADIUS Virtual Circuit (VC) Logging allows the Cisco 6400 Universal Access Concentrator to accurately record the virtual path interface (VPI) and virtual circuit interface (VCI) of an incoming subscriber session.

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.

A new command to display the VPI/VCI information that can be used by the RADIUS VC Logging feature has been added.

Configuring RADIUS VC Logging

Perform the following tasks to configure RADIUS VC logging:

- Configuring the NME Interface IP Address on the NSP
- Verifying the NME Interface IP Address
- Configuring RADIUS VC Logging on the NRP
- Verifying RADIUS VC Logging
- Selecting the IP Address for RADIUS Attribute 4 (NAS-IP Address)

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



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.

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 subnet 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#
```

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

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."

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 7-1 to configure an IP address for that interface.

Table 7-1 RADIUS Global Configuration Commands and Selected IP Addresses

Global Configuration Commands			Selected IP Address
<code>ip radius source-interface <int x></code>	<code>radius-server attribute nas-port format d</code>	<code>radius-server attribute 4 nrp</code>	
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
<code>Router> show atm ingress [all local-vc vpi/vci] [detailed]</code>	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. The CPE uses the subnet mask to calculate an IP address pool from which IP addresses are assigned to PCs using the access link.

Configuring the Subnet Mask

Choose at least one of the following methods to configure the subnet mask that the NRP will pass to the CPE upon request:

- Configuring the Subnet Mask in the RADIUS User Profile
- Configuring the Subnet Mask on the NRP



Note

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

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.

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

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
```

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 <i>number</i>	Creates or specifies the virtual template interface. Enters interface configuration mode.
Step 2	Router(config-if)# ppp ipcp mask <i>subnet-mask</i>	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

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 aal5cisco ppp 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.

Configuring IPCP Subnet Mask Support on the CPE

Some CPE is hard-coded to request the subnet mask from the peer. If, however, the CPE uses one of the following operating systems, you must configure the CPE to support and initiate IPCP subnet mask negotiation:

- Cisco Internetwork Operating System (Cisco IOS)
- Cisco Broadband Operating System (CBOS)



Note

Make sure you check and follow the documentation for your CPE software release. The following sections provide typical configuration guidelines for enabling CPE to support subnet mask negotiation.

Cisco Internetwork Operating System (Cisco IOS)

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 <i>type number</i>	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.



Note

The **ppp ipcp mask request** command is currently supported in Cisco IOS Release 12.1(3)DC, and will be supported in Cisco IOS Release 12.1(5)T.

Example

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

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

Cisco Broadband Operating System (CBOS)

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

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
NNTTP 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 Tips

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 **ip local pool** command in global configuration mode:

Command	Purpose
Router(config)# ip local pool <i>pool-name start-IP</i> [<i>end-IP</i>] [group <i>group-name</i>] [cache-size <i>size</i>]	Configures a group of local IP address pools, gives this group a name, and specifies a cache size.

Example: 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
```

This example specifies pool group “grp1” consisting of pools “p1_g1”, “p2_g1” and “p3_g1”; pool group “grp2” consisting of pools “p1_g2”, “p2_g2”; and pools “lp1” and “lp2” which are members of the base system group. Note the overlap addresses: IP address 1.1.1.1 is in all of them (“grp1” group, “grp2” group and the base system group). Also note that there is no overlap within any group (including the base system group, which is unnamed).

This example shows pool names that provide an easy way to associate a pool name with a group (when the pool name stands alone). While this may be an operational convenience, there is no required relationship between the names used to define a pool and the name of the group.

Verifying Local Pool Groups for IP Overlapping Address Pools

To verify that the new pool groups exist, enter the **show ip local pool group** command and check for the pool group name in the output.

This new command acts exactly like the existing command if the new **group** keyword is not present.

Command	Purpose
Router(config)# show ip local pool [[group group-name] pool-name]	Configures a group of local IP address pools and gives this group a name.

The forms of this **show** command allow the following:

show ip local pool - displays all pools

show ip local pool poolname - displays only pool *poolname*

show ip local pool group - displays all pools in base system group

show ip local pool group group-name - displays all pools in a group

The following example displays all pools:

```
router#sh ip local pool
Pool          Begin          End            Free   In use
** pool <p1> is in group <g1>
p1            10.1.1.1      10.1.1.10     10     0
              10.1.1.21     10.1.1.30     10     0
** pool <p2> is in group <g2>
p2            10.1.1.1      10.1.1.10     10     0
lc11         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#
```

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

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

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

Configuring Extended ATM PVC Trap Support

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

Command	Purpose
<pre>Router(config)# snmp-server enable traps atm pvc extension {up down oam failure loopback}</pre>	<p>Enables the sending of extended ATM PVC traps. The keywords are as follows:</p> <ul style="list-style-type: none"> • 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.

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	<pre>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}]</pre>	Specifies the ATM interface using the appropriate form of the interface atm command. ¹
Step 4	<pre>Router(config-if)# pvc [name] vpi/vci</pre>	Enables the PVC.
Step 5	<pre>Router(config-if-atm-vc)# oam-pvc manage</pre>	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.

Configuring Extended ATM PVC Trap Support Example

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# <code>debug atm errors</code>	Displays ATM errors.
Router# <code>debug atm oam</code>	Displays information about ATM OAM events.
Router# <code>debug snmp packets</code>	Displays information about every SNMP packet sent or received by the router.



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

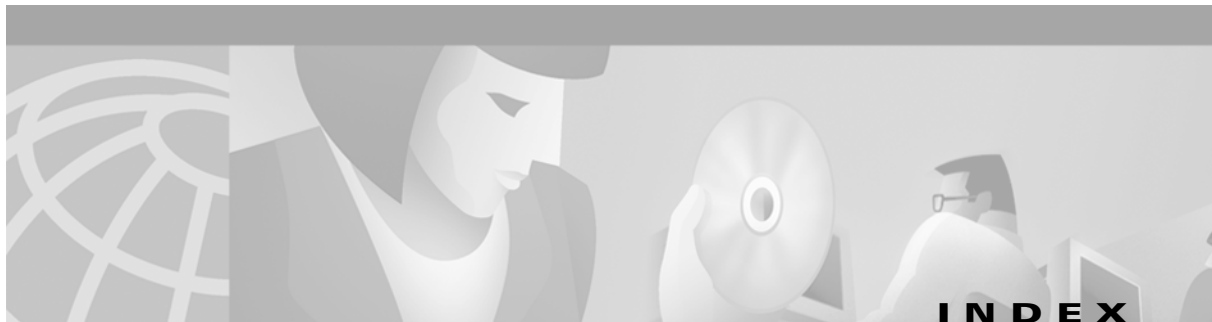
- VC** See Virtual Connection.
- VCI** virtual channel identifier. 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through a series of ATM switches on its way to its destination. ATM switches use the VPI/VCI fields 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 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.



A

AAA authentication

configuring for PPP 5-13

aaa authentication command 4-13

aaa authentication ppp command 5-14

aaa authorization command 4-13

aaa new-model command 4-13, 5-14

AAA server group support for proxy services

configuring 4-32

verifying 4-33

accept dialin command 2-3

Access-Accept message 4-4, 4-5

access control list

see ACL

Access-Reject message 4-4

Access-Request message 4-5, 4-40

Account-Info attributes 4-40

service group profiles 4-57

user profiles 4-43

accounting records

Account Logoff 4-35

Account Logon 4-35

attributes 4-37

Connection Start 4-36

Connection Stop 4-36

Account Logoff accounting record 4-35, 4-66

Account Logon accounting record 4-35

ACL

downstream 4-40, 4-43, 4-47, 4-48, 4-59

packet filtering 4-6

upstream 4-40, 4-43, 4-47, 4-59

ADSL 4-38

asynchronous transfer mode

see ATM

ATM interface

configuring PPPoE 5-6

ATM RBE

benefits 6-3

configuration examples 6-4

configuring 6-4

restrictions 6-4

verifying 6-5

attr command 4-12

authentication

local 5-14

RADIUS 5-14

TACACS+ 5-15

Auto Service attribute 4-41, 4-43, 4-44

B

bridging

(examples) 6-2

configuring 6-1

RFC 1483 example 6-2

C

CEF

configuring 4-17

L2TP scalability prerequisite 2-1

restrictions 4-10

verifying 4-17

Cisco 6400 4-2, 4-8

Cisco 6400 Software Setup Guide 4-8

- Cisco-AVPair attributes
 - list of **4-40**
 - PTA-MD **4-6**
 - service profiles **4-47, 4-48**
 - Transparent Passthrough Filter pseudo-service profile **4-59**
 - user profiles **4-43**
 - VPDN **4-20**
- Cisco Express Forwarding
 - see CEF
- Cisco Service Selection Dashboard
 - see Cisco SSD
- Cisco SESM
 - Group Description attribute **4-57**
 - overview **4-1**
 - proxy service **4-5**
 - PTA-MD **4-6**
 - Service User attribute **4-37, 4-42**
 - SSG default network **4-13**
- Cisco SSD
 - required version for single host login **4-11**
- Cisco Subscriber Edge Services Manager
 - see Cisco SESM
- clear ssg connection command **4-67**
- clear ssg host command **4-67**
- clear ssg next-hop command **4-67**
- clear ssg pass-through-filter command **4-67**
- clear ssg service command **4-67**
- clear vpdn tunnel l2tp command **6-9**
- concurrent access **4-42, 4-46, 4-47, 4-54**
- concurrent service access mode **4-7**
- configuring
 - AAA server group support for proxy services **4-32**
 - ATM RBE **6-4**
 - bridging **6-1**
 - CEF **4-17**
 - default network **4-13**
 - fastswitching **4-15**
 - host key **4-28**
 - IPCP subnet mask
 - on CPE **6-11**
 - L2TP **2-2**
 - LAC to communicate with RADIUS server **2-5**
 - LNS **4-21**
 - local forwarding **4-23**
 - local pool group for IP OAP **6-14**
 - local service profiles **4-12**
 - MPLS **3-2**
 - MPLS VPNs **3-7**
 - NAT **4-17**
 - NME interface IP address on NSP **6-6**
 - NRP as LAC **4-19**
 - NRPs as MPLS edge LSRs, connecting through VPI range **3-5**
 - NRPs as MPLS edge LSRs and connecting through PVP **3-3**
 - open garden **4-24**
 - PPP **5-1**
 - AAA authentication **5-3**
 - PPP autosense **5-9**
 - PPPoA **5-2**
 - PPPoE **5-5**
 - virtual template **5-5**
 - PPPoE on ATM interface **5-6**
 - PPP virtual template **5-2**
 - proxy RADIUS enhancements **4-33**
 - RADIUS profile for domain preauthorization **2-6**
 - RADIUS profile for tunnel service authorization **2-6**
 - RADIUS profiles **4-39**
 - pseudo-service profiles **4-59**
 - service group profiles **4-56**
 - service profiles **4-46**
 - SSG L2TP **4-19**
 - user profiles **4-42**
 - RADIUS VC logging **6-6**
 - RADIUS VC logging on NRP **6-7**
 - routing **6-1**
 - security **4-13**

sessions per tunnel limiting LAC 2-9
 sessions per tunnel limiting RADIUS profile 2-10
 SSG features 4-11
 SSG interfaces 4-14
 SSG multicast 4-16
 SSG RADIUS interim accounting 4-16
 SSG services 4-15
 SSG with L2TP Service Type 4-19
 subnet mask 6-9
 on NRP 6-10
 RADIUS user profile 6-10
 TCP Redirect - Logon 4-26
 tunnel sharing in RADIUS profile 2-13
 tunnel sharing LAC 2-12
 VPDN on the LAC 2-2
 VPDN on the LNS 2-3
 VPI/VCI indexing to service profile 4-18
 Connection Start accounting record 4-36
 Connection Stop accounting record 4-36, 4-66
 control channel parameters 6-8
 Control-Info attributes 4-42
 conventions xiv

D

debug radius command 4-68
 default network 4-4, 4-6
 configuring 4-13
 example 4-63
 verifying 4-14
 Digital Subscriber Line Access Multiplexers
 (DSLAMs) 4-2
 DNS 4-41, 4-46, 4-47, 4-50, 4-51
 DNS redirection 4-7
 DNS Server Address attribute 4-41, 4-47, 4-50
 documentation, obtaining xv
 document conventions xiv
 Domain Name attribute 4-41, 4-47, 4-53

domain name system
 see DNS
 domain preauthorization
 configuring RADIUS profile 2-6
 enabling 2-5
 example 2-8
 RADIUS user profile 2-6
 example 2-8
 tunnel service authorization step 2-4
 downlink interface 4-5, 4-14
 downstream ACL attribute 4-40, 4-43, 4-47, 4-48, 4-59

E

enabling
 domain preauthorization 2-5
 SSG 4-12
 VPDN and multihop functionality 2-16
 encapsulation command 2-3
 extended high system availability (EHSA) 4-8

F

fastswitching
 configuring 4-15
 example 4-65
 verifying 4-16
 Full Username Attribute 4-33, 4-41, 4-47, 4-51

G

Group Description attribute 4-41, 4-57

H

hold-queue

- command **6-3**
- configuring limits **6-3**
- default limits (table) **6-2**
- input **6-2**
- output **6-2**
- verifying limits **6-3**

host key

- benefits **4-8**
- configuring **4-28**
- monitoring and troubleshooting **4-31**
- prerequisites **4-11**
- restrictions **4-10**
- verifying **4-31**

IIdle-Timeout attribute **4-7, 4-43, 4-48**IGMP **4-5**

- SSG multicast **4-16**

inac1 attribute **4-6, 4-40, 4-43, 4-44, 4-47, 4-49, 4-60**

ingress tunnel name

- mapping to LNS **2-17**
- VPDN tunnel authorization search by **2-17**

initiate-to command **2-9**

input hold-queue limit

- configuring **6-3**
- default **6-2**
- description **6-2**
- verifying **6-3**

interface atm command **6-18**

interfaces

- configuring for SSG **4-14**
- example **4-63**
- verifying for SSG **4-14**

interface virtual-template command **2-3, 5-2**

Internet Group Management Protocol

see IGMP

IOS NAT

example **4-66**

IP

routing

- (examples) **6-2**
- configuring **6-1**

ip cef command **2-1, 4-17**

IPCP subnet mask

- configuring support on CPE **6-11**
- CBOS **6-12**
- IOS **6-12**
- overview **6-9**
- troubleshooting **6-13**
- verifying support on CPE **6-13**

ip dhcp-server command **5-2**IP hint **4-6**ip local pool command **5-2**

IP MTU

setting **5-6**

ip nat command **4-18**

IP OAP

configuring local pool group **6-14**

IP QoS and PPP call rate **6-2**ip radius source-interface command **6-8**ip unnumbered command **5-2**ip unnumbered ethernet command **2-3**

K

keepalive command **6-6**

keepalive interval

definition **6-5**

interface

configuring **6-6**

default **6-5**

verifying **6-6**

L2TP tunnel

configuring **6-7**

default **6-5**

verifying **6-7**

L

L2F **2-1**

L2TP

configuring **2-2**

configuring LNS **4-21**

configuring SSG with L2TP Service Type **4-19**

monitoring **2-20, 4-23**

overview **2-1**

restrictions **2-1**

SSG example **4-21**

SSG prerequisites **4-11**

troubleshooting **2-20**

L2TP access concentrator

see LAC

L2TP control channel parameters **6-8**

L2TP network server

see LNS

L2TP scalability

prerequisites **2-1**

restrictions **2-1**

L2TP scalability configuration example **6-10**

l2tp tunnel hello command **6-7**

l2tp tunnel nosession-timeout command **6-10**

L2TP Tunnel Password attribute **4-40, 4-47**

l2tp tunnel receive-window command **6-9**

l2tp tunnel retransmit command **6-8**

L2TP tunnel service authorization

example **2-7**

restrictions **2-1**

L2TP tunnel switching

example **2-18**

overview **2-14**

restrictions **2-1**

L2TP tunnel timeout

configuring **6-10**

defaults **6-10**

verifying **6-10**

label switch router

see MPLS edge LSR

LAC

configuring NRP as **4-19**

configuring sessions per tunnel limiting on **2-9**

configuring to communicate with RADIUS server **2-5**

configuring VPDN on **2-2**

Layer 2 service

selection **4-12**

Layer 2 tunnel protocol

see L2TP

Layer 3 service

selection **4-11**

prerequisites **4-11**

LCP

definition **6-3**

session initiations

limiting simultaneous **6-4**

overview **6-3**

verifying limits **6-4**

lcp max-load-metric command **6-4**

lcp max-session-starts command **6-4**

LDAP **4-1, 4-4**

Lightweight Directory Access Protocol

see LDAP

Link Control Protocol

See LCP

LNS

configuring

SSG 4-21

configuring VPDN on 2-3

local authentication 5-14

local control channel receive window size

configuring 6-9

verifying 6-9

local forwarding

configuring 4-23

example 4-23

verifying 4-23

local pool groups

configuring for IP OAP 6-14

verifying 6-15

local-profile command 4-12

local service profiles

configuring 4-12

example 4-65

verifying 4-12

M

maintaining

PPP autosense (table) 5-13

PPPoE 5-9

RADIUS VC logging 6-9

mapping ingress tunnel name to LNS 2-17

max services

example 4-65

memory, recommended

L2TP scalability 2-2

monitoring

host key 4-31

L2TP 4-23

PPP autosense (table) 5-13

PPPoE 5-9

RADIUS VC logging 6-9

SSG 4-67

VPDN and L2TP 2-20

VPI/VCI indexing to service profile 4-19

monitoring, maintaining commands

VPDN (table) 2-21

MPLS

configuring 3-2

configuring VPNs 3-7

prerequisites 3-1

restrictions 3-1

MPLS edge LSRs

configuring NRPs as

connecting through PVP 3-3

connecting through VPI range 3-5

MTU Size Attribute 4-20, 4-41, 4-47

multicast

benefits 4-5

configuring for SSG 4-16

example 4-65

verifying for SSG 4-16

multihop

enabling 2-16

multiprotocol label switching

see MPLS

N

NAT 4-6

configuring 4-17

proxy service 4-5

verifying 4-18

Network Address Translation

see NAT

network management ethernet

see NME

next hop gateway 4-42, 4-48

Next Hop Gateway attribute 4-7, 4-42, 4-48

Next Hop Gateway pseudo-service profile 4-61

Next Hop Gateway Table Entry attribute **4-42, 4-61**

next hop key **4-42, 4-48, 4-54, 4-61**

next-hop table

example **4-64**

NME interface IP address

configuring on NSP **6-6**

verifying **6-7**

non-PPP network **4-7**

non-PPP user **4-4**

NRP

authentication **5-13**

local **5-14**

RADIUS **5-14**

TACACS+ **5-15**

O

OAM enhancements **6-15**

OAM management

enabling **6-18**

oam-pvc command **6-18**

OAP

benefits **6-14**

example **6-14**

overview **6-13**

restrictions **6-14**

verifying local pool groups **6-15**

objectives, document **xiii**

Octets Input attribute **4-38**

Octets Output attribute **4-38**

open garden

configuring **4-24**

restrictions **4-10**

outacl attribute **4-6, 4-40, 4-43, 4-47, 4-48, 4-59**

output hold-queue limit

configuring **6-3**

default **6-2**

description **6-2**

verifying **6-3**

overlapping address pools

see OAP

P

passthrough service **4-5, 4-20, 4-42, 4-48, 4-55**

Password attribute **4-43, 4-48, 4-57**

peer default ip address pool command **5-2**

Point-to-Point Protocol

see PPP

port-bundle length

specifying **4-30**

PPP

AAA authentication

configuring **5-3, 5-13**

configuring **5-1**

configuring RADIUS server **5-14**

configuring TACACS+ server **5-15**

connect to SSG **4-14**

prerequisites **5-1**

restrictions **5-1**

specifying default authentication method **4-13**

ppp authentication command **2-3, 5-2**

PPP autosense

configuring **5-9**

example **5-10**

monitoring and maintaining (table) **5-13**

troubleshooting **5-13**

verifying **5-10**

PPPoA call rate and IP QoS **6-2**

PPPoA

(example) **5-4**

configuring **5-2**

configuring PVCs **5-3**

restrictions **5-1**

troubleshooting **5-4**

verifying **5-4**

virtual template **5-2**

PPPoE

- configuring 5-5
- configuring on ATM interface 5-6
- example 5-7
- monitoring and maintaining 5-9
- restrictions 5-1
- troubleshooting 5-9
- verifying 5-6
- pppoe limit max-sessions command 5-16
- pppoe limit per-mac command 5-16
- pppoe limit per-vc command 5-16
- pppoe limit per-vlan command 5-16
- pppoe max-sessions command 5-16
- PPPoE session count MIB
 - configuring 5-19
 - objects and tables (table) 5-20
- PPPoE session limit
 - configuring 5-15
- PPP Termination Aggregation
 - see PTA
- ppp timeout authentication command 6-5
- ppp timeout retry command 6-5
- PPP timeouts
 - authentication
 - default 6-4
 - overview 6-4
 - configuring 6-5
 - retry
 - default 6-4
 - overview 6-4
 - verifying 6-5
- PPP virtual template
 - configuring 5-2
- PPTP 2-1
- precloning virtual access interfaces
 - configuring 6-7
 - overview 6-7
 - restrictions 6-2
 - verifying 6-8

prerequisites

- L2TP for SSG 4-11
- L2TP scalability 2-1
- Layer 3 service selection 4-11
- MPLS 3-1
- PPP 5-1
- SSG 4-11
- proxy RADIUS enhancements
 - configuring 4-33
 - example 4-33
 - restrictions 4-10
 - verifying 4-34
- proxy service 4-5, 4-20, 4-42, 4-44, 4-48, 4-52, 4-55
- pseudo-service profile 4-6
 - Next Hop Gateway 4-61
 - Transparent Passthrough Filter 4-59, 4-60
- pseudo-service profiles
 - configuring 4-59
- PTA 4-6
- PTA-MD 4-6
- PTA multi-domain
 - see PTA-MD

R

RADIUS

- accounting records 4-34
 - Account Logoff 4-35, 4-66
 - Account Logon 4-35
- attributes 4-37
 - Connection Start 4-36
 - Connection Stop 4-36, 4-66
- attributes
 - Account-Info 4-40, 4-43, 4-57
 - Auto Service 4-41, 4-43, 4-44
 - Cisco-AVPair 4-6, 4-40, 4-43, 4-47
 - Control-Info 4-42
 - DNS Server Address 4-41, 4-47, 4-50
 - Domain Name 4-7, 4-41, 4-47, 4-53

- Full Username Attribute 4-33, 4-47, 4-51
- Group Description 4-41, 4-57
- Idle-Timeout 4-4, 4-7, 4-43, 4-48
- MTU Size Attribute 4-20, 4-41, 4-47
- Next Hop Gateway 4-42, 4-48
- Next Hop Gateway Table Entry 4-61
- Octets Input 4-38
- Octets Output 4-38
- Password 4-43, 4-48, 4-57
- RADIUS Server 4-6, 4-32, 4-42, 4-47, 4-52
- Service Authentication Type 4-47
- Service-Defined Cookie 4-33, 4-47, 4-53
- Service Description 4-42, 4-47, 4-53
- Service Group 4-41, 4-43, 4-45, 4-57
- Service-Info 4-41, 4-47
- Service Mode 4-42, 4-47, 4-54
- Service Name 4-37, 4-41, 4-42, 4-43, 4-44, 4-57, 4-58
- Service Next Hop Gateway 4-54
- Service Route 4-6, 4-42, 4-48, 4-54
- Service-Type 4-48, 4-57
- Service User attribute 4-37
- Session-Timeout 4-4, 4-7, 4-43, 4-48
- Standard 4-43, 4-48, 4-57
- Type of Service 4-42, 4-48, 4-55
- configuring NRP to use 5-14
- transparent passthrough 4-5, 4-6
- troubleshooting 4-68
- RADIUS Attribute 4
 - global configuration commands and selected IP addresses (table) 6-9
 - selecting IP address for 6-8
- RADIUS Attribute 8 4-6
- RADIUS interim accounting
 - configuring for SSG 4-16
 - example 4-66
 - verifying for SSG 4-17
- RADIUS profiles
 - configuring for SSG 4-39
 - configuring for SSG L2TP 4-19
- RADIUS server
 - communicating with LAC 2-5
 - configuring for PPP 5-14
- RADIUS Server attribute 4-6, 4-32, 4-42, 4-47, 4-52
- radius-server attribute 4 nrp command 6-8
- radius-server attribute nas-port command 5-14
- radius-server command 2-5, 4-13
- radius-server host command 5-14
- radius-server key command 5-14
- RADIUS VC logging 6-6
 - configuring 6-6
 - configuring on NRP 6-7
 - monitoring and maintaining 6-9
 - verifying 6-8
- RBE for CEF 6-5
- receive window size
 - configuring 6-9
 - verifying 6-9
- redundancy
 - example 4-65
 - SSG 4-8
- Remote Access Dial-In User Service
 - see RADIUS
- request dialin command 2-2
- restrictions
 - ATM RBE 6-4
 - CEF 4-10
 - L2TP
 - scalability 2-1
 - tunnel service authorization 2-1
 - tunnel switching 2-1
 - MPLS 3-1
 - OAP 6-14
 - open garden 4-10
 - PPPoA 5-1
 - PPPoE 5-1
 - proxy RADIUS enhancements 4-10
 - single host login 4-11
 - SSG 4-10

VPI/VCI indexing to service profile **4-10**

RFC 1483 encapsulation

- bridging **6-2**
- IP routing **6-3**

routed bridge encapsulation

- see RBE

routing

- (examples) **6-2**
- configuring **6-1**
- IP example **6-3**

RWS

- configuring **6-9**
- verifying **6-9**

S

security

- configuring **4-13**
- example **4-63**
- verifying **4-13**

selecting

- IP Address for RADIUS Attribute 4 **6-8**

sequential access **4-42, 4-46, 4-47, 4-54**

sequential service access mode **4-7**

service access mode **4-7**

service access order **4-6**

Service Authentication Type attribute **4-47**

Service-Defined Cookie attribute **4-33, 4-42, 4-47, 4-53**

Service Description attribute **4-42, 4-47, 4-53**

Service Group attribute **4-41, 4-43, 4-45, 4-57**

service group profiles

- Account-Info attributes **4-57**
- configuring **4-56**
- example **4-58**
- Standard attributes **4-57**

Service-Info attributes **4-41**

- service profiles **4-47**

Service Mode attribute **4-42, 4-47, 4-54**

Service Name attribute **4-37, 4-41, 4-42, 4-43, 4-44, 4-57, 4-58**

Service Next Hop Gateway attribute **4-54**

service profiles

- attributes **4-46**
- Cisco-AVPair attributes **4-47**
- configuring **4-46**
- example **4-56**
- Service-Info attributes **4-47**
- Standard attributes **4-48**

Service Route attribute **4-42, 4-48, 4-54**

services

- configuring for SSG **4-15**
- example **4-64**
- verifying for SSG **4-15**

service search order

- example **4-64**

Service Selection Gateway

- see SSG

Service-Type attribute **4-48, 4-57**

Service User attribute **4-37, 4-42**

sessions per tunnel limiting **2-9**

- configuring LAC **2-9**
- configuring RADIUS profile **2-10**
- example **2-9**
- RADIUS service profile

 - example **2-11**

Session-Timeout attribute **4-7, 4-43, 4-48**

setting

- IP MTU **5-6**

shared secret **4-13**

show atm pvc ppp command **5-4**

show interface virtual-access command **5-4**

show ip cef command **4-17**

show ip nat translations command **4-18**

show running-config command **4-12, 4-13, 4-14, 4-15, 4-16, 4-17, 4-18, 4-19**

show ssg binding command **4-67**

show ssg connection command **4-67**

show ssg direction command **4-14, 4-67**

show ssg host command **4-67**

- show ssg next-hop command **4-15, 4-67**
- show ssg pass-through-filter command **4-67**
- show ssg service command **4-15, 4-67**
- show ssg vc-service-map command **4-19**
- show vpdn tunnel all
 - new field descriptions (table) **2-20**
- show vpdn tunnel all command **2-20, 6-9, 6-12**
- show vtemplate command **6-8**
- Simple Network Management Protocol
 - see SNMP
- single host login **4-11**
 - restrictions **4-11**
- SNMP **4-3, 4-5**
- SSG
 - Account-Info attributes **4-40**
 - benefits **4-4**
 - CEF
 - configuring **4-17**
 - verifying **4-17**
 - Cisco-AVPair attributes **4-40**
 - configuration example **4-62**
 - CEF **4-66**
 - default network **4-63**
 - fastswitching **4-65**
 - interfaces **4-63**
 - IOS NAT **4-66**
 - local service profile **4-65**
 - max services **4-65**
 - multicast **4-65**
 - next-hop table **4-64**
 - RADIUS interim accounting **4-66**
 - redundancy **4-65**
 - security **4-63**
 - services **4-64**
 - service search order **4-64**
 - transparent passthrough filter **4-65**
 - configuring features **4-11**
 - Control-Info attributes **4-42**
 - default network
 - configuring **4-13**
 - verifying **4-14**
 - enabling **4-12**
 - fastswitching
 - configuring **4-15**
 - verifying **4-16**
 - interfaces
 - configuring **4-14**
 - verifying **4-14**
 - L2TP
 - configuring RADIUS profiles **4-19**
 - example **4-21**
 - monitoring **4-23**
 - local forwarding
 - configuring **4-23**
 - example **4-23**
 - verifying **4-23**
 - monitoring and troubleshooting **4-67**
 - multicast
 - configuring **4-16**
 - verifying **4-16**
 - NAT
 - configuring **4-17**
 - verifying **4-18**
 - NRP DRAM required for L2TP **4-11**
 - open garden
 - configuring **4-24**
 - overview **4-1**
 - prerequisites **4-11**
 - proxy RADIUS enhancements
 - configuring **4-33**
 - example **4-33**
 - verifying **4-34**
 - pseudo-service profiles
 - configuring **4-59**
 - RADIUS
 - troubleshooting **4-68**

- RADIUS interim accounting
 - configuring 4-16
 - verifying 4-17
 - RADIUS profiles
 - configuring 4-39
 - redundancy 4-8
 - restrictions 4-10
 - security
 - configuring 4-13
 - verifying 4-13
 - service group profiles
 - configuring 4-56
 - service profiles
 - configuring 4-46
 - services
 - configuring 4-15
 - verifying 4-15
 - single host login 4-11
 - TCP Redirect - Logon
 - configuring 4-26
 - verifying 4-27
 - user profiles
 - configuring 4-42
 - VPI/VCI indexing to service profile
 - configuring 4-18
 - monitoring 4-19
 - verifying 4-19
 - VSAs 4-40
 - web selection 4-4
 - with L2TP Service Type 4-19
 - ssg accounting interval command 4-17
 - ssg bind direction command 4-14
 - ssg bind service command 4-15
 - ssg default-network command 4-13
 - ssg fastswitch command 4-15
 - ssg maxservice command 4-15
 - ssg multicast command 4-16
 - ssg next-hop command 4-67
 - ssg next-hop download command 4-15
 - ssg pass-through command 4-67
 - ssg radius-helper command 4-13
 - ssg service-password command 4-13
 - ssg service-search-order command 4-15
 - ssg vc-service-map command 4-18
 - Standard attributes
 - service group profiles 4-57
 - service profiles 4-48
 - user profiles 4-43
 - static domain name
 - configuring 2-4
 - PVC example 2-7
 - VC class example 2-7
 - verifying 2-5
 - sticky IP 4-6
 - subnet mask
 - configuring 6-9
 - on NRP 6-10
 - RADIUS user profile 6-10
 - verifying
 - on NRP 6-11
 - RADIUS User Profile 6-10
-
- T**
- TACACS+ 4-5, 5-15
 - TACACS+ server
 - configuring for PPP 5-15
 - tacacs-server host command 5-15
 - tacacs-server key command 5-15
 - TCP Redirect - Logon
 - configuring 4-26
 - verifying 4-27
 - technical assistance xvi
 - terminating tunnel from LAC 2-16
 - Transmission Control Protocol/Internet Protocol (TCP/IP) 4-7
 - transparent passthrough 4-5, 4-6, 4-59

- transparent passthrough filter
 - example [4-65](#)
- Transparent Passthrough Filter pseudo-service profile [4-59, 4-60](#)
 - Cisco-AVPair attributes [4-59](#)
- troubleshooting
 - host key [4-31](#)
 - IPCP subnet mask [6-13](#)
 - PPP autosense [5-13](#)
 - PPPoA [5-4](#)
 - PPPoE [5-9](#)
 - SSG [4-67](#)
 - RADIUS [4-68](#)
 - VPDN and L2TP [2-20](#)
- troubleshooting commands
 - VPDN (table) [2-21](#)
- tunnel service authorization
 - configuring RADIUS profile [2-6](#)
 - enhancements [2-4](#)
 - LAC example [2-8](#)
 - RADIUS service profile [2-6](#)
 - example [2-8](#)
- Tunnel Share attribute [2-13](#)
- tunnel sharing [2-12](#)
 - configuring LAC [2-12](#)
 - configuring RADIUS profile [2-13](#)
- Type of Service attribute [4-42, 4-48, 4-55](#)

U

- uplink interface [4-5, 4-14](#)
 - binding services to [4-15](#)
- upstream ACL attribute [4-40, 4-43, 4-47, 4-59](#)
- user profiles
 - Account-Info attributes [4-43](#)
 - attributes [4-42](#)
 - Cisco-AVPair attributes [4-43](#)
 - configuring [4-42](#)
 - example [4-46](#)

- Standard attributes [4-43](#)

V

- vendor-specific attributes
 - see VSAs
- verifying
 - AAA server group support for proxy services [4-33](#)
 - ATM RBE [6-5](#)
 - CEF [4-17](#)
 - default network [4-14](#)
 - fastswitching [4-16](#)
 - host key [4-31](#)
 - local forwarding [4-23](#)
 - local pool groups for IP OAP [6-15](#)
 - local service profiles [4-12](#)
 - NAT [4-18](#)
 - NME interface IP address [6-7](#)
 - PPP autosense [5-10](#)
 - PPPoA [5-4](#)
 - PPPoE [5-6](#)
 - proxy RADIUS enhancements [4-34](#)
 - security [4-13](#)
 - SSG enabled [4-12](#)
 - SSG interfaces [4-14](#)
 - SSG multicast [4-16](#)
 - SSG RADIUS interim accounting [4-17](#)
 - SSG services [4-15](#)
 - TCP Redirect - Logon [4-27](#)
 - VPI/VCI indexing to service profile [4-19](#)
- virtual access interfaces [2-3](#)
- virtual access interfaces, precloning
 - configuring [6-7](#)
 - overview [6-7](#)
 - restrictions [6-2](#)
 - verifying [6-8](#)
- virtual circuits
 - see VCs

- virtual private dial-up network
 - see VPDN
- virtual template interface **2-3**
- virtual-template pre-clone command **6-7**
- virtual templates **5-2**
 - configuring for PPPoE **5-5**
 - static IP assignment (caution) **5-2**
- VPDN **2-2**
 - enabling **2-16**
 - monitoring **2-20**
 - monitoring, maintaining commands (table) **2-21**
 - troubleshooting commands (table) **2-21**
- vpdn enable command **2-2, 2-16**
- VPDN Group attribute **2-13**
- vpdn group command **2-2**
- VPDN IP Address attribute **4-40, 4-47**
- VPDN IP Addresses attribute **2-10**
- VPDN IP Address Limits attribute **2-11**
- vpdn multihop command **2-16**
- VPDN tunnel authorization searches by ingress tunnel name **2-17**
- VPDN Tunnel ID attribute **4-40, 4-47**
- VPI/VCI indexing to service profile
 - configuring **4-18**
 - monitoring **4-19**
 - restrictions **4-10**
 - verifying **4-19**
- VSA s **4-5, 4-13**
 - SSG **4-40**
 - SSG (table) **4-40**

W

- web selection **4-4**