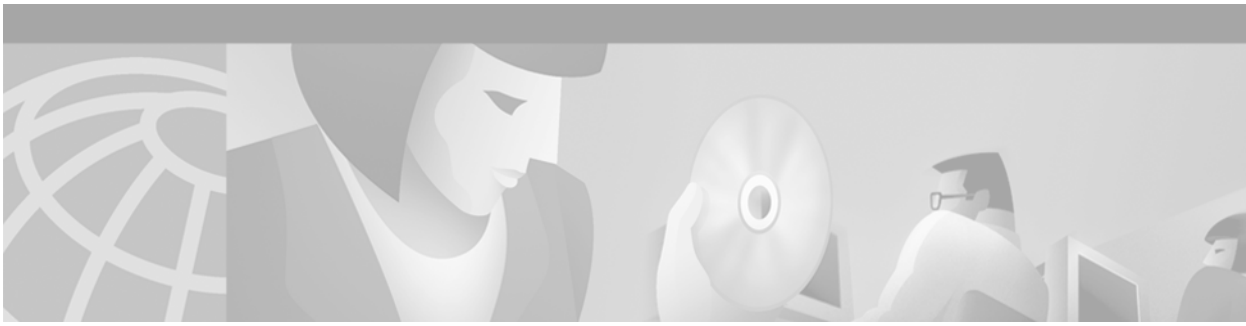


Release Notes for Cisco 6400 for Cisco IOS Release 12.2 B

October 8, 2001

Cisco IOS Release 12.2(2)B

OL-1650-01

Note This release is supported on the Cisco 6400 NRP-1 only. The NRP-2 is currently supported by Cisco IOS Release 12.1(5)DC. The Cisco 6400 NSP is currently supported by Release 12.1(5)DB. Cisco IOS Release 12.2(2)B support on the NRP-1 is compatible with Release 12.1(5)DB support on the NSP.

Note You can find the most current Cisco IOS documentation on Cisco.com. This set of electronic documents might contain updates and modifications made after the hard-copy documents were printed.

These release notes for the Cisco 6400 describe the enhancements provided in Cisco IOS Release 12.2(2)B. This release is based on Cisco IOS Release 12.2(2) T1 and reflects a combination of prior Releases 12.1(5)DB and 12.1(5)DC for the Cisco 6400. All features included in releases 12.1(5)DB and 12.1(5)DC are included in this release. For information about releases 12.1(5)DB and 12.1(5)DC, refer to:

http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/relnotes/index.htm

For a list of the software caveats that apply to Release 12.2(2)B, see the "Software Caveats" section on page 27 and *Caveats for Cisco IOS Release 12.2 T*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Use these release notes in conjunction with the cross-platform *Release Notes for Cisco IOS Release 12.2* T located on Cisco.com and the Documentation CD-ROM.

Note In these release notes, the acronym NRP refers to both the NRP-1 and the NRP-2. Where there are differences between the NRP-1 and the NRP-2, a clear distinction is made.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

These release notes describe the following topics:

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(2)B and includes the following sections:

Memory Recommendations

Table 1 lists the memory recommendations for the Cisco 6400.

Note Release 12.2(2)B supports the NRP-1 images only.

Table 1 Memory Recommendations for the Cisco 6400

Product Name	Description	Image Names	Recommended Minimum DRAM Memory	Recommended Minimum Flash Memory
Both	Boot Image	c6400r-boot-mz	Not applicable	Not applicable
NRP-2	IOS NRP-2 BASE IOS NRP-2 MULTIDOMAIN IOS NRP-2 WEB SELECTION	c6400r2sp-g4p5-mz	256 MB for up to 6500 sessions 512 MB for over 6500 sessions	Not applicable

Table 1 Memory Recommendations for the Cisco 6400 (continued)

Product Name	Description	Image Names	Recommended Minimum DRAM Memory	Recommended Minimum Flash Memory
NRP-1	IOS NRP-1 BASE IOS NRP-1 MULTIDOMAIN IOS NRP-1 WEB SELECTION	c6400r-g4p5-mz	64 MB for up to 750 sessions 128 MB for over 750 sessions	8 MB
NSP		c6400s-wp-mz c6400s-html.tar	The standard 64 MB DRAM memory configuration supports up to 12K virtual circuits (VCs). 128 MB DRAM is recommended for supporting up to 32K VCs, or for using ATM RMON or ATM Accounting. 128 MB DRAM is also recommended for an upgrade from an earlier release to Cisco IOS Release 12.1(5)DB.	20 MB or 32 MB [1] 350 MB recommended for NRP-2 configurations

1. The 20 MB Flash Disk is no longer available; the 32 MB Flash Disk is now the default Flash configuration.

Note In most NRP-2 configurations, 256 MB DRAM is adequate for up to 6500 sessions. More sessions require 512 MB DRAM.

Note In most NRP-1 configurations, 64 MB DRAM is adequate for up to 750 sessions. More sessions require 128 MB DRAM. Using the NRP-1, for an upgrade from an earlier release to Cisco IOS Release 12.2(2)B, 128 MB DRAM is recommended.

Supported Hardware

Cisco IOS Release 12.2(2)B supports the Cisco 6400 NRP-1 module.

The Cisco 6400 NSP and the NSP with Stratum 3/BITS (NSP-S3B) are supported by Cisco IOS Release 12.1(5)DB. The NSP-S3B, otherwise identical to the NSP, is required to use the Building Integrated Timing Supply (BITS) Network Clocking software feature. The Cisco 6400 NRP-2 is supported by Cisco IOS Release 12.1(5)DC.

Software Compatibility

Release 12.2(2)B on the NRP-1 is compatible with Release 12.1(5)DB on the NSP. You can upgrade the NRP-1 to Release 12.2(2)B while using Release 12.1(5)DB for the NSP. Cisco recommends that you upgrade to Release 12.2(2)B for the NSP when this support becomes available.

For NRP-Service Selection Gateway (SSG) users, Cisco IOS Release 12.2(2)B works with the Cisco Service Selection Dashboard (SSD) version 2.5(1) and 3.0(1) and Subscriber Edge Services Manager (SESM) 3.1(1).

Determining the Software Version

To determine the version of Cisco IOS software currently running on the Cisco 6400 NRP-1, log in to the NRP-1 and enter the **show version** EXEC command:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) C6400R Software (C6400R-G4P5-M), Version 12.2(2)B
```

To determine the version of Cisco IOS software currently running on the Cisco 6400 NSP, log in to the NSP and enter the **show version** EXEC command:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) C6400 Software (C6400S-WP-M), Version 12.1(5)DB
```

The output from these commands includes additional information, including processor revision numbers, memory amounts, hardware IDs, and partition information.

Upgrading to a New Software Release

For information about upgrading software on the Cisco 6400, including upgrading a single- or dual-NRP system to a new software release, see the software note *Upgrading Software on the 6400 UAC* located at http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/softnote/upgradsw.htm

For general information about upgrading to a new software release, see the product bulletin *Cisco IOS Upgrade Ordering Instructions* located at http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm

If you do not have an account on Cisco.com and want general information about upgrading to a new software release, see the product bulletin *Cisco IOS Software Release 11.3 Upgrade Paths and Packaging Simplification (#703: 12/97)* on Cisco.com at:

Technical Documents: Product Bulletins: Software:Cisco IOS 11.3:
Cisco IOS Software Release 11.3 Upgrade Paths No. 703

This product bulletin does not contain information specific to Cisco IOS Release 12.2(2)B but provides generic upgrade information that may apply to Cisco IOS Release 12.2(2)B.

Feature Set Tables

The Cisco IOS software is packaged in software images. Each image contains a specific set of Cisco IOS features.

Table 3 lists the features supported by the Cisco 6400 NRP-1 images in this release. This table also provides information for features supported by earlier releases, and features supported by earlier releases on the NRP-2.

Note This table might not be cumulative or list all the features in each image. You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after hard-copy documents were printed. For a list of the T-train features in this platform, refer to Feature Navigator. For more information about Feature Navigator, see the "Feature Navigator" section on page 30.

Table 2 Features Supported by the Cisco 6400 NRP-1 in Cisco IOS Release 12.2(2)B

Feature	NRP-1 Supported as of Cisco IOS Release	NRP-2 Supported as of Cisco IOS Release
Access Protocols		
Integrated Routing and Bridging (IRB)	12.0(3)DC	12.1(4)DC
Multilink Point-to-Point Protocol (MLPPP or MLP)	12.1(3)DC	12.1(4)DC
PPP [1] IPCP [2] Subnet Negotiation	12.0(5)DC	12.1(4)DC
PPP over ATM (PPPoA) terminated	12.0(3)DC	12.1(4)DC
PPP over Ethernet (PPPoE) terminated	12.0(3)DC	12.1(4)DC
PPPoA/oE autosense (SNAP [3])	12.1(1)DC	12.1(5)DC
Remote Access into MPLS VPN	12.2(2)B	—
Routed bridge encapsulation (RBE)	12.0(5)DC	12.1(4)DC
RBE Subinterface Grouping	12.1(4)DC	12.1(4)DC
RBE unnumbered DHCP [4]	12.1(1)DC	12.1(4)DC
RBE with DHCP	12.0(5)DC	12.1(4)DC
RBE with DHCP Option 82	12.1(5)DC	12.1(5)DC
RFC 1483 bridging	12.0(3)DC	12.1(4)DC
RFC 1483 routing	12.0(3)DC	12.1(4)DC
VC [5] Traffic Shaping	12.0(3)DC	—
Aggregation and Virtual Private Networks (VPN)		
IP [6] Overlapping address pools (AOP)	12.1(5)DC	Not yet supported
L2TP [7] Multi-Hop	12.1(1)DC	12.1(4)DC
L2TP tunnel service authorization enhancement	12.1(1)DC	12.1(4)DC
L2TP tunnel sharing	12.1(1)DC	12.1(4)DC
L2TP tunnel switching [8]	12.1(1)DC	12.1(4)DC
MPLS [9] Edge Label Switch Router (Edge LSR)	12.0(7)DC	Not yet supported
MPLS Label Distribution Protocol	12.2(2)B	—
MPLS Label Switch Controller (LSC) for BPX	12.0(7)DC	Not yet supported
MPLS VPNs [10]	12.0(7)DC	—
PPPoA tunneled into L2TP	12.0(5)DC	12.1(4)DC
PPPoE tunneled into L2TP	12.0(5)DC	12.1(4)DC
Remote Access into MPLS VPN	12.1(5)DC	Not yet supported
RFC 1577	12.0(3)DC	12.1(4)DC
VLAN [11] (ISL [12]) on NRP	12.0(3)DC	12.1(4)DC
VLAN (802.1q) on NRP-2 GE[13]	Not applicable	12.1(5)DC
Configuration and Monitoring		
ATM[14] PVC [15] Range Command	12.1(4)DC	12.1(4)DC

Table 2 Features Supported by the Cisco 6400 NRP-1 in Cisco IOS Release 12.2(2)B (continued)

Feature	NRP-1 Supported as of Cisco IOS Release	NRP-2 Supported as of Cisco IOS Release
Per VC error display	12.1(3)DC	12.1(5)DC
Hardware Support		
ATM (OC-3, OC-12, DS3) Interfaces	12.0(3)DC	12.1(4)DC
FE [16] Interface: 10/100 auto-negotiation, auto-sensing	12.0(3)DC	Not applicable
GE Interface	Not applicable	12.1(5)DC
Network Management Ethernet (NME)	12.0(5)DC	12.1(4)DC
NRP 1+1 Redundancy	12.0(3)DC	—
IP and Routing		
Address Resolution Protocol (ARP)	12.0(3)DC	12.1(4)DC
Border Gateway Protocol version 4 (BGP4)	12.0(3)DC	12.1(4)DC
Enhanced Interior Gateway Routing Protocol (EIGRP)	12.0(3)DC	12.1(4)DC
Generic routing encapsulation (GRE)	12.0(3)DC	12.1(4)DC
Internet Group Management Protocol (IGMP)	12.0(3)DC	12.1(4)DC
Internet Protocol (IP) forwarding	12.0(3)DC	12.1(4)DC
IP multicast	12.0(3)DC	12.1(4)DC
IP QoS—Policing, Marking, and Classification	12.2(2)B	—
Intermediate System-to-Intermediate System (IS-IS)	12.0(3)DC	12.1(4)DC
Network Address Translation (NAT) support for NetMeeting Directory	12.0(3)DC	12.1(4)DC
NetFlow for RFC1483 into MPLS VPN	12.1(5)DC	Not yet supported
Open Shortest Path First (OSPF)	12.0(3)DC	12.1(4)DC
PIM [17] Dense Mode & Sparse Mode	12.0(3)DC	12.1(4)DC
Routing Information Protocol (RIP)/RIP v2	12.0(3)DC	12.1(4)DC
Transmission Control Protocol (TCP)	12.0(3)DC	12.1(4)DC
Telnet	12.0(3)DC	12.1(4)DC
Trivial File Transfer Protocol (TFTP)	12.0(3)DC	12.1(4)DC
Transparent Bridging	12.0(3)DC	12.1(4)DC
User Datagram Protocol (UDP)	12.0(3)DC	12.1(4)DC
Web Cache Coordination Protocol (WCCP) version 1	12.0(3)DC	12.1(4)DC
WCCP (v2)	12.0(7)DC	12.1(4)DC
Network Management		
PPPoE Session Count MIB	12.2(2)B	—
Simple Network Management Protocol (SNMP) (v1, v2, and v3)	12.0(3)DC	12.1(4)DC
RADIUS/AAA		

Table 2 Features Supported by the Cisco 6400 NRP-1 in Cisco IOS Release 12.2(2)B (continued)

Feature	NRP-1 Supported as of Cisco IOS Release	NRP-2 Supported as of Cisco IOS Release
Password Authentication Protocol (PAP)/Challenge Handshake Authentication Protocol (CHAP)	12.0(3)DC	12.1(4)DC
Remote Authentication Dial-In User Service (RADIUS)	12.0(3)DC	12.1(4)DC
RADIUS Attribute 8 (Framed-IP-Address) in Access Requests (IP Hint)	12.1(3)DC	12.1(4)DC
Terminal Access Controller Access Control System Plus (TACACS+) (admin login only)	12.0(3)DC	12.1(4)DC
VPI [18]/VCI [19] RADIUS Request and RADIUS Accounting for PPPoA	12.0(3)DC	12.1(5)DC
VPI/VCI in RADIUS Request and RADIUS Accounting for PPPoE	12.1(1)DC	12.1(5)DC
Scalability and performance		
GRE Cisco express forwarding (CEF)	12.1(1)DC	12.1(5)DC
LAC [20] CEF switching	12.1(3)DC	12.1(4)DC
L2TP sessions per tunnel limiting	12.1(1)DC	12.1(4)DC
NAT CEF switching	12.1(1)DC	12.1(4)DC
Per VC buffer management	12.1(1)DC	12.1(4)DC
PPPoA CEF	12.1(1)DC	12.1(4)DC
PPPoE Fast Switching for Multicast	12.1(1)DC	12.1(5)DC
RBE CEF switching	12.1(5)DC	12.1(5)DC
Service Selection Gateway (NRP-SSG)		
PPP Aggregation Termination over Multiple Domains (PTA-MD)	12.0(3)DC	12.1(4)DC
RADIUS Interim Accounting	12.0(5)DC	12.1(4)DC
SSG AAA Server Group for Proxy RADIUS	12.2(2)B	—
SSG Automatic Service Logon	12.0(3)DC	12.1(4)DC
SSG CEF Switching	12.0(5)DC	12.1(4)DC
SSG Default Network	12.0(3)DC	12.1(4)DC
SSG DNS [21] Fault Tolerance	12.0(3)DC	12.1(4)DC
SSG enable (default is disabled)	12.0(7)DC	12.1(4)DC
SSG full username RADIUS attribute	12.1(3)DC	12.1(4)DC
SSG Host Key	12.2(2)B	—
SSG HTTP [22] Redirect (Phase 1)	12.1(5)DC	12.1(5)DC
SSG Cisco IOS NAT support	12.0(5)DC	12.1(4)DC
SSG Local Forwarding	12.1(1)DC	12.1(5)DC
SSG Open Garden	12.1(5)DC	12.1(5)DC

Table 2 Features Supported by the Cisco 6400 NRP-1 in Cisco IOS Release 12.2(2)B (continued)

Feature	NRP-1 Supported as of Cisco IOS Release	NRP-2 Supported as of Cisco IOS Release
SSG Passthrough and Proxy Service	12.0(3)DC	12.1(4)DC
SSG Sequential and Concurrent Service	12.0(3)DC	12.1(4)DC
SSG Service Defined Cookie	12.1(3)DC	12.1(4)DC
SSG single host logon	12.1(3)DC	12.1(4)DC
SSG with GRE	12.0(3)DC	12.1(5)DC
SSG with Multicast	12.0(3)DC	12.1(4)DC
SSG with L2TP Service Type	12.0(7)DC	12.1(4)DC
TCP Redirect—Logon	12.2(2)B	—
VPI/VCI Static binding to a Service Profile	12.0(5)DC	12.1(4)DC
WebSelection	12.0(3)DC	12.1(4)DC
Other Features and Feature Enhancements		
Segmentation and Reassembly Buffer Management Enhancements	12.1(1)DC	Not applicable
Session Scalability Enhancements	12.2(2)B	—

1. PPP = Point-to-Point Protocol
2. IPCP = Internet Protocol Control Protocol
3. SNAP = Subnetwork Access Protocol
4. DHCP = Dynamic Host Configuration Protocol
5. VC = virtual circuit
6. IP = Internet Protocol
7. L2TP = Layer 2 Tunneling Protocol
8. In Cisco IOS Release 12.1(5)DC, L2TP tunnel switching for the NRP-2 has been tested and is supported at the same session and tunnel levels as the NRP-1. For more information, see Table 6 on page 25.
9. MPLS = Multiprotocol Label Switching
10. VPN = Virtual Private Network
11. VLAN = Virtual LAN
12. ISL = Inter-Switch Link
13. GE = Gigabit Ethernet
14. ATM = Asynchronous Transfer Mode
15. PVC = permanent virtual circuit
16. FE = Fast Ethernet
17. PIM = Protocol Independent Multicast
18. VPI = Virtual path identifier
19. VCI = Virtual channel identifier
20. LAC = L2TP access concentrator
21. DNS = Domain Name System
22. HTTP = Hypertext Transfer Protocol

The Cisco IOS software is packaged in software images. Each image contains a specific set of Cisco IOS features. Table 3 lists the features supported by the Cisco 6400 NSP image called c6400s-wp-mz in Cisco IOS Release 12.1(5)DB. Release 12.2(2)B does not support the NSP.

Note This table might not be cumulative or list all the features in each image. You can find the most current Cisco IOS documentation on Cisco.com. This set of electronic documents might contain updates and modifications made after the hard-copy documents were printed. If you have a Cisco.com login account, you can find image and release information regarding features prior to Cisco IOS Release 12.1(5)DB by using the Feature Navigator tool at http://www.cisco.com/go/fn.

Table 3 Features Supported by the Cisco 6400 NSP in Cisco IOS Release 12.1(5)DB

Feature	Supported as of Cisco IOS Release
ATM Connections	
F4 and F5 Operation, administration, and maintenance (OAM) cell segment and end-to-end flows	12.0(4)DB
Hierarchical virtual private (VP) tunnels	12.0(4)DB
Logical multicast support (up to 254 leaves per output port, per point-to-multipoint virtual circuits [VCs])	12.0(4)DB
Multipoint-to-point User-Network Interface (UNI) signaling	12.0(4)DB
Point-to-Point and Point-to-Multipoint VCs	12.0(4)DB
Permanent virtual circuit (PVC), Soft PVC, Soft permanent virtual path (PVP), and switched virtual circuit (SVC)	12.0(4)DB
Soft virtual channel connections (VCCs) and virtual path connections (VPCs)	12.0(4)DB
VC Merge	12.0(4)DB
VP and VC switching	12.0(4)DB
VP multiplexing	12.0(4)DB
VP tunneling	12.0(4)DB
ATM Internetworking	
LAN Emulation Server (LES) and LAN Emulation Configuration Server (LECS)	12.0(4)DB
RFC 1577 (Classical IP over ATM) ATM Address Resolution Protocol (ARP) server/client	12.0(4)DB
ATM Per-Flow Queuing	
Dual leaky bucket policing (ITU-T I.371and ATM Forum UNI specifications)	12.0(4)DB
Intelligent early packet discard (EPD)	12.0(4)DB
Intelligent partial (tail) packet discard	12.0(4)DB
Multiple, weighted (dynamic) thresholds for selective packet marking and discard	12.0(4)DB
Per-VC or per-VP output queuing	12.0(4)DB
Strict priority, rate, or weighted round robin scheduling algorithms	12.0(4)DB
ATM Traffic Classes	
Available bit rate (ABR) (EFCI [1] + RR [2]) + minimum cell rate (MCR)	12.0(4)DB
Constant bit rate (CBR)	12.0(4)DB
Per-VC or per-VP CBR traffic shaping	12.0(4)DB
Shaped CBR VP tunnels (up to 128)	12.0(4)DB
Substitution of other service categories in shaped VP tunnels	12.0(4)DB

Table 3 Features Supported by the Cisco 6400 NSP in Cisco IOS Release 12.1(5)DB (continued)

Feature	Supported as of Cisco IOS Release
Support for non-zero MCR on ABR connections	12.0(4)DB
Unspecified bit rate (UBR)	12.0(4)DB
UBR + MCR	12.0(4)DB
Variable bit rate-non-real time (VBR-NRT)	12.0(4)DB
VBR-real time (RT)	12.0(4)DB
Configuration and Monitoring	
ATM access lists on Interim Local Management Interface (ILMI) registration	12.0(4)DB
ATM soft restart	12.0(4)DB
PCMCIA[3] Disk Mirroring	12.1(5)DB
Per-VC or per-VP nondisruptive port snooping	12.0(4)DB
Hardware Support	
1+1 Slot Redundancy (EHSA [4])	12.0(4)DB
Network Management Ethernet (NME)	12.0(5)DB
NRP-2 support	12.1(4)DB
NSP 1+1 Redundancy	12.0(4)DB
Synchronous Optical Network (SONET) automatic protection switching (APS) support	12.0(4)DB
Stratum 3/BITS	12.0(7)DB
Telco alarms	12.0(4)DB
IP and Routing	
Dynamic Host Configuration Protocol (DHCP) client support	12.0(4)DB
Internet Protocol (IP)	12.0(4)DB
Network Time Protocol (NTP)	12.0(4)DB
Telnet	12.0(4)DB
Network Management	
ATM accounting enhancements	12.0(4)DB
ATM Accounting Management Information Base (MIB)	12.0(4)DB
ATM remote monitoring (RMON) MIB	12.0(4)DB
Signaling diagnostics and MIB	12.0(4)DB
Simple Network Management Protocol (SNMP)	12.0(4)DB
Web Console	12.0(4)DB
RADIUS/AAA	
Terminal Access Controller Access Control System Plus (TACACS+) (admin login only)	12.0(4)DB
Scalability and Performance	
Capability to view used/unused Input Translation Table (ITT) blocks	12.1(4)DB
Fragmentation minimization	12.1(4)DB

Table 3 Features Supported by the Cisco 6400 NSP in Cisco IOS Release 12.1(5)DB (continued)

Feature	Supported as of Cisco IOS Release
ITT block shrinking	12.1(4)DB
Signaling and Routing	
ATM Network Service Access Point (NSAP) and left-justified E.164 address support	12.0(4)DB
Closed user groups (CUGs) for ATM VPNs	12.0(4)DB
E.164 address translation and autoconversion	12.0(4)DB
Hierarchical Private Network Node Interface (PNNI)	12.0(4)DB
Interim-Interswitch Signaling Protocol (IISP)	12.0(4)DB
ILMI 4.0	12.0(4)DB
VPI/VCI [5] range support in ILMI 4.0	12.0(4)DB
UNI 3.0, UNI 3.1, and UNI 4.0	12.0(4)DB

1. EFCI = Explicit Forward Congestion Indication
2. RR = relative rate
3. PCMCIA = Personal Computer Memory Card International Association
4. EHSA = Enhanced High System Availability
5. VPI/VCI = virtual path identifier/virtual channel identifier

New and Changed Information

This section describes new features available in Release 12.2(2)B and enhancements to existing features offered in prior releases.

TCP Redirect—Logon

Note If using SESM or SSD as a captive portal, this feature requires Cisco SSD Release 3.0(1) or Cisco SESM.

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. For more information on this feature, refer to:

http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/feat_gd/12_2_2/fg2_ssg.htm

Configuring MPLS Virtual Private Networks

Virtual Private Networks (VPNs) provide the appearance, functionality, and usefulness of a dedicated private network. The VPN feature for MPLS allows a Cisco IOS network to deploy scalable IPv4 Layer 3 VPN backbone service with private addressing, controlled access, and service-level guarantees between sites.

VPNs create a private network environment within the public infrastructure. A service provider can use VPNs to target a given clientele and deliver individualized private network services to that clientele in a secure IP environment by using the public infrastructure.

For an overview of MPLS VPN and its benefits, refer to the *MPLS Virtual Private Networks* feature module.

Configuring MPLS VPN on a Cisco 6400

For general MPLS VPN configuration tasks, examples, and command references, see the *MPLS Virtual Private Networks* feature module.

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 of the *ATM Switch Router Software Configuration Guide.*

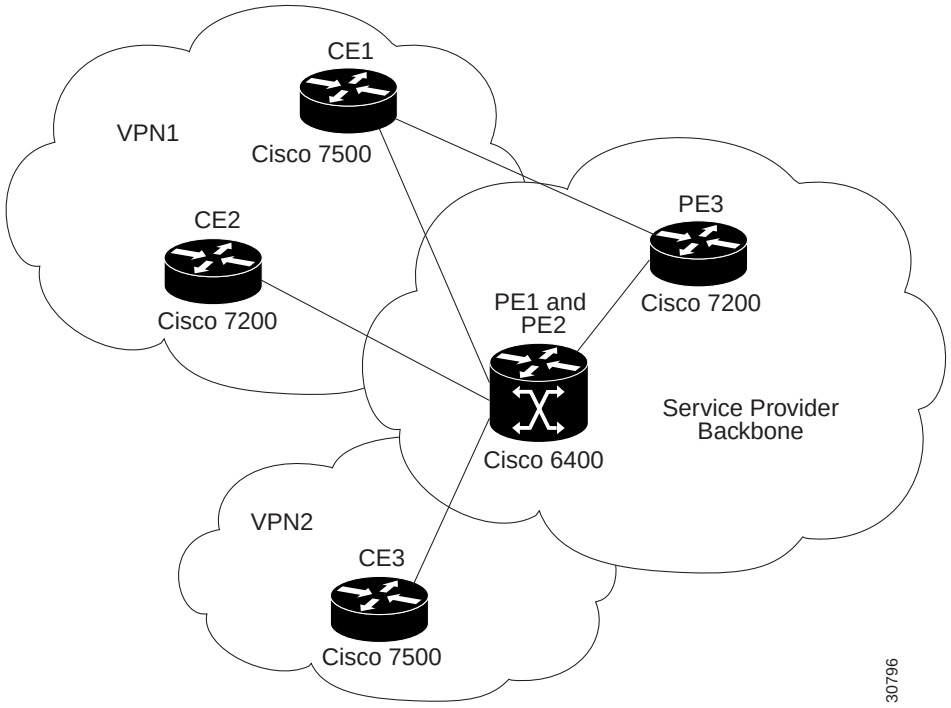
The examples in this section illustrate the configurations necessary to enable MPLS VPN on a Cisco 6400.

Basic MPLS VPN Configuration

This section presents a basic Cisco 6400 MPLS VPN configuration. As shown in Figure 1, 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 NRP-1 in the Cisco 6400, handles the CE1 portion of VPN1. PE2, or NRP-2 in the Cisco 6400, handles VPN2 as well as the CE2 portion of VPN1.

Figure 1 Basic Cisco 6400 MPLS VPN Topology



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

For more information, refer to:

http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/feat_gd/12_2_2/fg2_mpls.htm

MPLS Label Distribution Protocol

Cisco's MPLS label distribution protocol (LDP), as standardized by the Internet Engineering Task Force (IETF) and as enabled by Cisco IOS software, allows the construction of highly scalable and flexible IP Virtual Private Networks (VPNs) that support multiple levels of services.

LDP provides a standard methodology for hop-by-hop, or dynamic label, distribution in an MPLS network by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting labeled paths, called label switch paths or LSPs, forward label traffic across an MPLS backbone to particular destinations. These capabilities enable service providers to implement Cisco's MPLS-based IP VPNs and IP+ATM services across multivendor MPLS networks.

LDP provides the means for label switching routers (LSRs) to request, distribute, and release label prefix binding information to peer routers in a network. LDP enables LSRs to discover potential peers and to establish LDP sessions with those peers for the purpose of exchanging label binding information.

From an historical and functional standpoint, LDP is a superset of Cisco's prestandard Tag Distribution Protocol (TDP), which also supports MPLS forwarding along normally routed paths. For those features that LDP and TDP share in common, the pattern of protocol exchanges between network routing platforms is identical. The differences between LDP and TDP for those features supported by both protocols are largely embedded in their respective implementation details, such as the encoding of protocol messages, for example.

This release of LDP, which supports both the LDP and TDP protocols, provides the means for transitioning an existing network from a TDP environment to an LDP environment. Thus, you can run LDP and TDP simultaneously on any router platform. The routing protocol that you select can be configured on a per-interface basis for directly connected neighbors and on a per-session basis for nondirectly connected (targeted) neighbors. In addition, a label switch path (LSP) across an MPLS network can be supported by LDP on some hops and by TDP on other hops.

For more information, refer to this website:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ldp_221t.htm

IP QoS—Policing and Marking

Cisco IOS QoS offers two kinds of traffic regulation mechanisms—policing and shaping.

The rate-limiting features of committed access rate (CAR) and the Class-Based Policing features provide the functionality for policing traffic.

The features of Generic Traffic Shaping (GTS), Class-Based Shaping, Distributed Traffic Shaping (DTS), and Frame Relay Traffic Shaping (FRTS) provide the functionality for shaping traffic.

Release 12.2(2)B supports the Committed Access Rate (CAR) feature on NRP, which allows policing upstream/downstream subscriber traffic to specific rates. Additionally, traffic can be marked with specific IP Precedence. You can also use an access list (ACL) to classify traffic to be policed (and optionally marked).

For more details on CAR, refer to:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/cc111/car.pdf

Configurations

CAR can be configured on an interface or subinterface that has an IP address (or IP unnumbered Loopback). When configured on a virtual-template, it is applied to all the virtual-access interfaces derived from the template. Modifying the CAR parameters on the virtual template propagates the modification to the virtual-access interfaces.

To rate-limit or mark traffic from/to subscribers, you can configure upstream and/or downstream policing/marking as shown in the following examples (for more details, refer to the website mentioned earlier):

PPPoE/PPPoA termination—Configure CAR in the Virtual-Template

rate-limit output 256000 16000 32000 conform-action transmit exceed-action drop

This would restrict downstream traffic of each PPPoE (PPPoA) session to 256000 bits/sec. The burst size and excess burst size are 16000 bytes and 32000 bytes, respectively. Traffic exceeding the policing rate and burst are dropped.

rate-limit input 256000 16000 32000 conform-action set-prec-transmit 5 exceed-action set-prec-transmit 0

This sets the IP precedence bits in the IP header to 5 for packets that meet the policing rate. Exceeding packets are transmitted with IP precedence set to 0.

RBE interface—Configure CAR on the RBE Subinterface

```
interface ATM0/0/0.1001 point-to-point
  ip address 174.128.240.1 255.255.255.252
  rate-limit output 256000 16000 32000 conform-action transmit exceed-action drop
  atm route-bridged ip
  pvc 31/1001
    encapsulation aal5snap
```

1483 Routing—Configure CAR on the 1483 Routed Subinterface

```
interface ATM0/0/0.1005 point-to-point
  ip address 174.128.240.1 255.255.255.252
  rate-limit output 256000 16000 32000 conform-action transmit exceed-action drop
  pvc 31/1005
    encapsulation aal5snap
```

On the trunk side, you can configure upstream and/or downstream policing/marking by configuring CAR on an ATM subinterface, Fast Ethernet/Gigabit-Ethernet interface, or subinterface.

CAR is not supported on PPP/L2TP LAC at present, or on GRE tunnels.

Configuring Policing/Marking in RADIUS User Profile

For PPPoE/PPPoA sessions that terminate on NRP, instead of configuring CAR on the virtual template, you may configure CAR on the RADIUS user profile. This allows separate policing/marking on different PPPoE (PPPoA) sessions even though the sessions share the same virtual template. When the policing/marking parameters are defined on the AAA profile of a user, Cisco IOS software applies these policing/marking to any PPPoE (PPPoA) session established by the user.

The following AAA user profiles for John defines a policing rate of 120,000 bps. You can use any AAA server that supports Cisco AV pair (the following AAA configurations are for a Merit AAA Server).

john Password = “xyz”

Service-Type = Framed-User,

Framed-Protocol = PPP,

av-pair = “ip:addr-pool=pool4”,

av-pair = “lcp:interface-config#1=rate-limit output 256000 16000 32000 conform- action transmit exceed-action drop”

av-pair = “lcp:interface-config#2=rate-limit input 64000 16000 32000 conform-action transmit exceed-action drop”

Note The ' #1', '#2' need not be specified if there is only one “lcp:interface-config” AV-pair in the RADIUS user profile.

The “lcp:interface-config=” AV-pair takes the rest of the AV-pair string as a Cisco IOS command and applies it to the virtual-access interface when the user initiates the PPP session. For John, it therefore applies this command to the virtual-access interface:

rate-limit output 120000 16000 32000 conform-action transmit exceed-action drop

For AAA-based policing to work, you must configure the following in global configuration mode:

virtual-profile aaa

Verifying Policing/Marking

You can use the following command to verify CAR policing/marking:

show interface <int> rate-limit

Where <int> is any interface including virtual-access interface.

The above command displays the CAR configuration on the interface and policing statistics.

```
NRP1-s2-UUT# sh int Virtual-access 4 rate-limit
Virtual-Access4
  Output
    matches: all traffic
      params: 256000 bps, 16000 limit, 32000 extended limit
      conformed 335 packets, 459710 bytes; action: transmit
      exceeded 46 packets, 65851 bytes; action: drop
      last packet: 182368ms ago, current burst: 10017 bytes
      last cleared 00:05:22 ago, conformed 11000 bps, exceeded 1000 bps
```

Important Notes and Recommendations

1. Performance impact—CAR policing algorithm impacts performance due to its additional use of processor resource. Typical performance impact may be about 20 to 30%, although it would vary depending on the traffic mix and the configured protocol:
   - Packet Marking will additionally impact performance by about 2%
   - Using an ACL with CAR will affect performance depending on the type of ACL used

   Burst Size—The recommended configuration for burst size and excess burst size are as follows:

   Burst size = amount of traffic at the policed rate that can flow in one second interval (expressed in bytes)

   Excess burst = 2 x burst size

   For example, for a policing rate of 256,000 bps, you can choose burst = 32,000 (bytes), and excess burst = 64,000 (bytes). This will allow bursty traffic while maintaining an average policing rate of 256,000 bps. Smaller burst sizes will drop more packets for bursty traffic—larger burst sizes will better accommodate traffic bursts.

   For example, CAR configuration for 256 Kbps policing rate should be:

   rate-limit output 256000 32000 64000 conform-action transmit exceed-action drop

   However, if the traffic is not very bursty, then lower values of burst and excess-burst may work, but typically burst-size should not be less than 16,000 bytes for TCP traffic. You may need to experiment to find burst and excess bursts that best fit the traffic characteristics.
2. For PPPoE and PPPoA subscribers, you can configure the above rate-limit command in the virtual-template. If PPPoE is used, it is possible to use only one policing rate for all subscribers on an NRP (since only one virtual template is used in PPPoE). If PPPoA is used, it is possible to use multiple virtual templates with different policing rates on the same NRP. For 1483-routed and RBE cases, configure CAR on the ATM subinterface for the subscriber. Ensure that the subinterface has an IP address (either directly, or IP unnumbered interface).

3. CAR support with SSG is not available. Do not turn on SSG.
4. IP Policing is not applicable in PPP/L2TP case (on LAC) or on tunnel interfaces.
5. CAR works with CEF-switched packets, so do not configure fast or process switching for traffic to be policed. CAR doesn't officially support policing of packets locally generated by the router or any packets that aren't CEF-switched including multicast packets.
6. Unlike shaping that buffers packets exceeding the shaping rate (until its buffer is full) and transmits them later, policing drops packets that exceed the configured rate. So depending on the traffic volume and burstiness, policing may lead to larger numbers of packet drops compared to shaping.
7. Some applications, such as VoIP and streaming video, are sensitive to packet drops. CAR should not be configured so that it can drop traffic of such applications. However, CAR can be used if the application completely downloads a voice/audio file before playing it.
8. AAA download of policing parameters—If you download policing parameters from a AAA server, the downloaded command string is parsed during PPP session establishment, which reduces the number of PPP sessions that can be established per second. The maximum number of PPP calls per second will be less than 10, depending on the PPP parameters configured in the virtual-template (ppp keepalive, authentication/retry timeouts), the number of configured sessions, and the traffic volume.
9. For scaling to a large number of PPPoE/PPPoA sessions, you should tune the ppp keepalive and authentication/retry timeouts according to scalability guidelines by appropriate configuration of ppp keepalive, ppp timeout retry, and ppp timeout authentication statements in the virtual-template. This is particularly important if you configure CAR policing parameters in AAA user profile.
10. The rate-limit command in a RADIUS user profile must not exceed 240 characters (which is sufficient for configuring any kind of policing and marking). If it does, the router may give errors or crash.

For more information on this feature, see the *Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2*, “Policing and Shaping” chapter.

Remote Access to MPLS VPN

The Remote Access to Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) solution integrates dial, Digital Subscriber Line (DSL), and cable remote access technologies into an MPLS VPN. For more information about the Remote Access to MPLS VPN integration solution, refer to the Remote Access to MPLS VPN Integration Solution documentation:

http://cco/univercd/cc/td/doc/product/vpn/solution/rampls/index.htm

Per-VC Traffic Shaping

The NRP-1 supports the unspecified bit rate (UBR) and variable bit rate non-real time (VBR-NRT) quality of service (QoS) classes.

Note You can specify only one QoS class per PVC. When you enter a new QoS class, it replaces the existing one.

The NRP-2 supports the VBR-NRT QoS class. When using VBR-NRT on the NRP-2, you might need to modify the ATM SAR transmission ring limit to provide more buffering space and time for packets on one or more VCs. For more information, see the **tx-ring-limit** command reference entry in the *Cisco 6400 Command Reference*.

Note If you do not specify a QoS class for a PVC, the PVC defaults to UBR, with a peak rate set to the maximum physical line speed.

For more information on this feature, see the *Cisco 6400 Software Setup Guide*, "Basic NRP Configuration" chapter, "Configuring PVC Traffic Shaping" section.

For Release 122.(2)B, the supported number of shaped VCs is:

- NRP-1—2000 VCs
- NRP-2SV—Not supported in this release
- NRP-2—Not supported in this release

PPPoE Session Count MIB

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

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

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

Table 4 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).

Table 4 PPPoE Session Count MIB Objects and Tables

Object	Description
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.

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.

For more information on this feature, see the *Cisco 6400 Feature Guide—Release 12.2.(2)B*, "Point-to-Point Protocol" chapter.

PPPoE Session Limit

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 a potential problem because the router might 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.

For more information on this feature, see the *Cisco 6400 Feature Guide—Release 12.2.(2)B*, "Point-to-Point Protocol" chapter.

ATM SNMP Trap and OAM Enhancements

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

ATM PVC traps are now:

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

ATM PVC UP Trap

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

ATM PVC OAM Failure Trap

The ATM SNMP Trap and OAM enhancements also introduce the ATM PVC OAM failure trap. OAM loopback is a mechanism that detects whether a connection is UP or DOWN by sending OAM end-to-end loopback command/response cells.

An OAM loopback failure indicates that the PVC has lost connectivity. The ATM PVC OAM failure trap is generated when OAM loopback for a PVC fails and is sent at the end of the notification interval.

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

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

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

Extended ATM PVC Traps

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

The extended traps include:

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

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

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

For more information on this feature, see the *Cisco 6400 Software Setup Guide,* "SNMP, RMON, and Alarm Configuration" chapter.

SSG AAA Server Group for Proxy RADIUS

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 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 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 more information on this feature, see the *Cisco 6400 Feature Guide—Release 12.2.(2)B*, "Service Selection Gateway" chapter.

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

- 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

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.

For more information on this feature, see the *Cisco 6400 Feature Guide—Release 12.2.(2)B*, "Service Selection Gateway" chapter.

Limitations and Restrictions

Cisco IOS Release 12.2(2)B supports only the Cisco 6400 NRP-1 module. The Cisco 6400 NRP-2 is supported by Release 12.1(5)DC, and the NSP is supported by Release 12.1(5)DB.

Important Notes

Session Scalability Commands

Table 6 shows the number of sessions and tunnels supported for the NRP-1 module in Cisco IOS Release 12.2(2)B. The numbers shown for the NRP-2 are not yet supported, but should be available in a future release. While using NRP-SSG, Cisco IOS Release 12.2(2)B supports the number of sessions and tunnels shown for NRP-1 in Table 7.

Table 6 Session and Tunnel Scalability in Cisco IOS Release 12.2(2)B

	NRP-1		NRP-2 (not yet supported)	
Protocol	**Supported Sessions**	**Supported Tunnels**	**Supported Sessions**	**Supported Tunnels**
L2TP PPPoA	up to 1700	up to 300	up to 8000	up to 2000
L2TP PPPoE	up to 2000	up to 300	up to 8000	up to 2000
L2TP Tunnel Switch PPPoA	up to 940	up to 50 Ingress up to 10 Egress		
L2TP Tunnel Switch PPPoE	up to 940	up to 50 Ingress up to 10 Egress		
PPPoA	up to 2000	—	up to 8000	—
PPPoE	up to 2000	—	up to 8000	—
PPP Autosense	up to 2000	—	up to 4000	—
RBE	up to 2000	—	up to 8000	—
RFC 1483 IP Routed	up to 2000	—	up to 8000	—
RFC1483 MPLS VPN	—	—	up to 4000	up to 500
RBE MPLS VPN	—	—	up to 4000	up to 500

Table 7 NRP-SSG Session and Tunnel Scalability in Cisco IOS Release 12.2(2)B

	NRP-1		NRP-2 (not yet supported)	
Protocol with NRP-SSG	**Supported Sessions**	**Supported Tunnels**	**Supported Sessions**	**Supported Tunnels**
L2TP PPPoA	up to 700	up to 100	up to 4000	up to 2000
L2TP PPPoE	up to 700	up to 100	up to 4000	up to 2000
PPPoA	up to 2000	—	up to 8000	—
PPPoE	up to 2000	—	up to 8000	—
RBE	up to 2000	—	up to 8000	—
RFC 1483 IP Routed	up to 2000	—	up to 8000	—
GRE PPPoA	—	—	up to 8000	up to 2000

Note To support more than 750 sessions, the NRP-1 must have 128 MB DRAM.

Note In most NRP-2 configurations, 256 MB DRAM is adequate for up to 6500 (PPPoE) sessions. More sessions require 512 MB DRAM.

Scalability Parameters

This section provides scalability tuning parameter values used during testing for 8000 PPPoA sessions and 2000 L2TP tunnels. These parameters prevent known issue CSCdu86416 from happening.

```
interface Virtual-Template1
keepalive 200
ppp timeout retry 25
ppp timeout authentication 20

vpdn-group 1
l2tp tunnel hello 150
l2tp tunnel receive-window 500
l2tp tunnel nosession-timeout 20
l2tp tunnel retransmit retries 12
l2tp tunnel retransmit timeout min 4
l2tp tunnel retransmit timeout max 6
```

Following is the hold-queue CLI used during testing.

```
interface ATM0/0/0
 no ip address
 load-interval 30
 atm vc-per-vp 2048
 no atm ilmi-keepalive
 hold-queue 4096 in
 hold-queue 4096 out
end
```

Note In most NRP-2 configurations, 256 MB DRAM is adequate for up to 6500 (PPPoE) sessions. More sessions require 512 MB DRAM.

Note The default threshold at which Cisco IOS declares a process to have run "too long" is too short for some Cisco IOS processes, when very large numbers of sessions are established on the NRP-2. Use the command **scheduler max-task-time 20000** to increase the default threshold. This will avoid unnecessary "CPUHOG" messages.

DHCP Option 82 Support for Routed Bridge Encapsulation

The DHCP Option 82 Support for RBE feature provides support for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option (Option 82) when using ATM RBE.

Service providers are increasingly using ATM RBE to configure DSL access. The DHCP Option 82 Support for RBE feature enables those service providers to use DHCP to assign IP addresses and DHCP Option 82 to implement IP address assignment policies such as limiting the number of IP addresses on specific ports on specific ports or ATM VCs.

The DHCP Relay Agent Information Option enables a DHCP relay agent to insert information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement IP address or other parameter-assignment policies.

The DHCP Option 82 Support for RBE feature uses a suboption of the DHCP Relay Agent Information Option called Agent Remote ID. The Agent Remote ID suboption enables the DHCP relay agent to report the ATM RBE subinterface port information to the DHCP server when a DHCP IP address request is processed through the ATM RBE subinterface. The DHCP server can use the ATM RBE subinterface information for making IP address assignments and security policy decisions.

Software Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

All caveats in Cisco IOS Release 12.2(2) T1 are also in Cisco IOS Release 12.2(2)B.

For information on caveats in Cisco IOS Release 12.2 T, see the *Caveats for Cisco IOS Release 12.2 T*, which lists severity 1 and 2 caveats and select severity 3 caveats and is located on Cisco.com and the Documentation CD-ROM.

Note Cisco IOS Release 12.2(2)B is in synchronization with Cisco IOS Release 12.2(2)T1.

Caveat numbers and brief descriptions are listed in Table 9. For details about a particular caveat, go to Bug Toolkit at:

http://www.cisco.com/kobayashi/bugs/bugs.html

To access this location, you must have an account on Cisco.com. For information about how to obtain an account, go to the "Feature Navigator" section on page 30.

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, go to Cisco.com and press **Login.** Then go to **Software Center: Cisco IOS Software: Cisco Bugtool Navigator II**. Another option is to go to http://www.cisco.com/support/bugtools/.

Open Caveats—Release 12.2(2)B

All the caveats listed in Table 8 are open in Cisco IOS Release 12.2(2)B for Cisco 6400 NRP-1. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 8 Open Caveats for Cisco 6400 NRP-1 for Release 12.2(2)B

Caveat ID Number	Description
CSCdm92848	EHSA minor alarm pop up after 2 non-redundancy NRP boot up
CSCdp59354	egress traffic to RBE ints process sw w/ FE+ISL & <<bridge irb>>
CSCdu01557	NRP crashes with BADFREEMAGIC message
CSCdu09764	c6400:NRP crash w/ bad magic on allocated block

Table 8 Open Caveats for Cisco 6400 NRP-1 for Release 12.2(2)B (continued)

Caveat ID Number	Description
CSCdu56256	%AMDP2_FE-3-UNDERFLO:causes interface to bounce
CSCdu64354	Option 82 and Radius VPI/VCI authentication does not work with S-PVC
CSCdv07110	NRP crash with BADMAGIC and BADBLOCK
CSCdv19996	NRP-1 FE port drop packets
CSCdv34094	Software forced crash from use of output modifiers
CSCdv45514	Bus error at chunk_free
CSCdv47420	NRP-1 ethernet interface does not get dynamic ip address
CSCdr04534	PPPoA/L2TP:2000 sess, some connected routes are not est after flap
CSCdr50376	Some sessions drop when the VCs are oversubscribed
CSCdr82324	L2TP:VPDN:Releasing idb for LAC/LNS tunnel
CSCds57906	6400NRP:crash in SYS-3-MGDTIMER
CSCdt74755	NAT cause high CPU utilization
CSCdp05523	NAT:Large address range & portlist chains cause cpu spikes

Closed and Resolved Caveats—Release 12.2(2)B

All the caveats listed in Table 9 are closed or resolved in Cisco IOS Release 12.2(2)B for Cisco 6400 NRP-1. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 9 Closed or Resolved Caveats for Release 12.2(2)B for Cisco 6400 NRP-1

Caveat ID Number	Description
CSCdp74289	In RBE, NRP uses Very Big buffers for outgoing packets of size 1500
CSCdp74444	paste large files via telnet hangs the router
CSCdt39140	high cpu when telnet has a zero send window and data to send
CSCds61231	RBE unnumbered does not work with IOS DHCP Server
CSCds79395	NRP crashes with %SYS-3-BADMAGIC in nat
CSCdt05069	6400NRP cannot send RADIUS-Attribute8(framed-ip-address) of PPPoA
CSCdt44101	NRP crashed while experiencing neighbor up and down
CSCdt45145	OAM-managed PVCs Stop Transmitting Data after NSP Failover
CSCdt47374	SNMP polling of virtual access interface crashes at cca_own_cb
CSCdt47730	OSPF and XtagATM interface issues on NRP when NSP reloads
CSCdt65265	Large sessions dropped on NRPx with SSG-L2TP under traffic
CSCdt67753	Need knob to disable automatic MTU adjustment added via CSCdr01713
CSCdt69743	memory leak problem
CSCdt69881	memory leak, memory allocation failure

Related Documentation

The following sections describe the documentation available for the Cisco 6400. Documentation is available online on Cisco.com and the Documentation CD-ROM.

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.2 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes*

  On Cisco.com at:

  Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Release Notes

  On the Documentation CD-ROM at:

  Cisco IOS Software Configuration: Cisco IOS Release 12.1: Release Notes

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:

  Technical Documents

- *Caveats for Cisco IOS Release 12.2* and *Caveats for Cisco IOS Release 12.2 T*

  As a supplement to the caveats listed in the "DHCP Option 82 Support for Routed Bridge Encapsulation" section in these release notes, see *Caveats for Cisco IOS Release 12.2* and *Caveats for Cisco IOS Release 12.2 T*, which contain caveats applicable to all platforms for all maintenance releases of Release 12.2.

  On Cisco.com:

  Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Release Notes: Caveats

  On the Documentation CD-ROM:

  Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.2**: **Caveats**

Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on Cisco.com at **Service & Support: Online Technical Support: Software Bug Toolkit** or at http://www.cisco.com/support/bugtools/.

Platform-Specific Documents

The documents listed in this section are available for the Cisco 6400 on Cisco.com and the Documentation CD-ROM.

To access Cisco 6400 documentation on Cisco.com, follow this path:

Technical Documents: Documentation Home Page: Aggregation Solutions: Cisco 6400 Universal Access Concentrator

To access Cisco 6400 documentation on the Documentation CD-ROM, follow this path:

Aggregation Solutions: Cisco 6400 Universal Access Concentrator

Platform-Specific Documents

- *Cisco 6400 Software Setup Guide*
- *Cisco 6400 Command Reference*
- *Cisco 6400 Feature Guide*
- *Cisco 6400 Hardware Installation and Maintenance Guide*
- *Cisco 6400 Installation and Replacement of Field-Replaceable Units*
- *Regulatory Compliance and Safety Information for the Cisco 6400*
- *Cisco 6400 Site Planning Guide*

Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image.

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to http://www.cisco.com/register and follow the directions to establish an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. It contains feature information about mainline-, T-, S-, and P-trains. You can access Feature Navigator at the following URL:

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

Cisco IOS Release 12.2 Documentation Set

Table 10 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in both electronic and printed form.

Note You can find the most current Cisco IOS documentation on Cisco.com and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2

Table 10 Cisco IOS Release 12.2 Documentation Set

Books	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Cisco IOS User Interfaces File Management System Management
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2*	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSw+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
• *Cisco IOS Dial Technologies Configuration Guide* • *Cisco IOS Dial Technologies Command Reference*	Preparing for Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Dial-on-Demand Routing Configuration Dial Backup Configuration Dial Related Addressing Service Virtual Templates, Profiles, and Networks PPP Configuration Callback and Bandwidth Allocation Configuration Dial Access Specialized Features Dial Access Scenarios

Table 10 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
• *Cisco IOS IP Configuration Guide* • *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services* • *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* • *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*	IP Addressing and Services IP Routing Protocols IP Multicast
• *Cisco IOS AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk Novell IPX
• *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide* • *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Cisco IOS Voice, Video, and Fax Configuration Guide* • *Cisco IOS Voice, Video, and Fax Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation

Table 10 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	ATM Broadband Access Frame Relay SMDS X.25 and LAPB
• *Cisco IOS Mobile Wireless Configuration Guide* • *Cisco IOS Mobile Wireless Command Reference*	General Packet Radio Service
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Debug Command Reference* • *Cisco IOS Software System Error Messages* • *New Features in 12.2 T-Based Limited Lifetime Releases* • *New Features in Release 12.2 T T* • *Release Notes* (Release note and caveat documentation for 12.2 T-based releases and various platforms)	

Obtaining Documentation

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

World Wide Web

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

http://www.cisco.com

Translated documentation is available at the following URL:

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

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

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

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

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

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

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

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

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

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

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

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

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

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

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

http://www.cisco.com

Technical Assistance Center

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

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

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

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

Cisco TAC Web Site

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

http://www.cisco.com/tac

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

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

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

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

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

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

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

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

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 29.