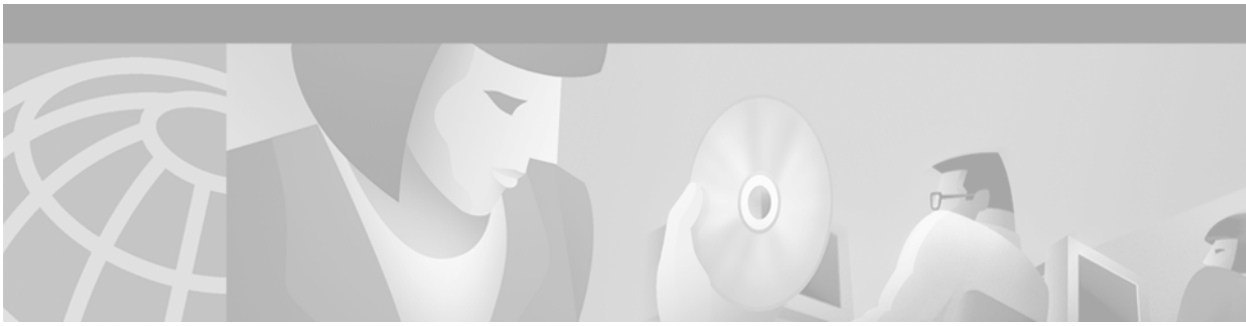

Release Notes for Cisco 6400 for Cisco IOS Release 12.2(4)B3

April 12, 2002

Cisco IOS Release 12.2(4)B3

OL-1650-03

Note You can find the most current Cisco IOS documentation on Cisco.com. This set of electronic documents contains the latest updates and modifications.

These release notes for the Cisco 6400 describe the enhancements provided in Cisco IOS Release 12.2(4)B3. This release is based on Cisco IOS Release 12.2(2)B5, which in turn is based on 12.2(4)T1 and reflects a combination of prior Releases 12.2(2)B, 12.1(5)DB, and 12.1(5)DC for the Cisco 6400. All features included in Cisco IOS Release 12.2(2)B and Cisco IOS Release 12.2(2)B5, as well as Cisco IOS Releases 12.1(5)DB and 12.1(5)DC, are included in this release. For information about these releases, refer to:

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

If you have a Cisco 6400 running a Cisco IOS Release 12.2(2)B and you are upgrading to Release 12.2(4)B3, refer to Table 5 on page 29 for a summary of important configuration differences.

For a list of the software caveats that apply to Release 12.2(4)B3, see the "Software Caveats" section on page 34 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 the NRP-1, NRP-2, and NRP-2SV. Where there are differences among the NRP types, a clear distinction is made.

Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/770/index.shtml. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/770/index.shtml.

CISCO SYSTEMS

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(4)B3 and includes the following sections:

Memory Recommendations

Table 1 lists the memory recommendations for the Cisco 6400.

Table 1 Memory Recommendations for the Cisco 6400

Product Name	Description	Image Names	Recommended Minimum DRAM Memory	Recommended Minimum Flash Memory
NRP	Boot Image	c6400r-boot-mz	Not applicable	Not applicable
NRP-2 and NRP-2SV	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 When running multicast in an NRP-2 configuration, the NRP-2 should have 512 MB of memory.

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(4)B3, 128 MB DRAM is recommended.

Supported Hardware

Cisco IOS Release 12.2(4)B3 supports the Cisco 6400 NRP-1, NRP-2, NRP-2SV, NSP, and NSP-S3B modules. The NSP-S3B, otherwise identical to the NSP, is required to use the Building Integrated Timing Supply (BITS) Network Clocking software feature.

Software Compatibility

For NRP-Service Selection Gateway (SSG) users, Cisco IOS Release 12.2(4)B3 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, log in to the NRP 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(4)B3
```

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 12.2(4)B3
```

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 "Upgrading Software on the Cisco 6400" appendix in the *Cisco 6400 Software Setup Guide* located at http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/sw_setup/index.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(4)B3 but provides generic upgrade information that may apply to Cisco IOS Release 12.2(4)B3.

Feature Set Tables

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

Table 2 lists the features supported by the Cisco 6400 NRP images in this release. Table 3 lists the features supported by the Cisco 6400 NSP images in this release. These tables also include features supported by earlier releases.

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 44.

Table 2 Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.2(4)B3

Feature	NRP-1 Supported as of Cisco IOS Release	NRP-2 Supported as of Cisco IOS Release	NRP-2SV Supported as of Cisco IOS Release
Access Protocols			
Enhancements to DHCP Option 82 Support for RBE	12.2(4)B3	12.2(4)B3	12.2(4)B3
Integrated Routing and Bridging (IRB)	12.0(3)DC	12.1(4)DC	12.2(2)B1
Multilink Point-to-Point Protocol (MLPPP or MLP)	12.1(3)DC	12.1(4)DC	12.2(2)B1
Per-VC[1] Traffic Shaping	12.0(3)DC	—	12.2(2)B1
PPP [2] IPCP [3] Subnet Negotiation	12.0(5)DC	12.1(4)DC	12.2(2)B1
PPPoE over Ethernet (FE[4] for NRP-1)	12.2(4)B3	—	—
PPPoE over Ethernet (GE for NRP-2SV only)	—	—	12.2(4)B3
PPP over ATM[5] (PPPoA) terminated	12.0(3)DC	12.1(4)DC	12.2(2)B1
PPP over Ethernet (PPPoE) terminated	12.0(3)DC	12.1(4)DC	12.2(2)B1
PPPoEoE with VLAN	12.2(4)B3	—	12.2(4)B3
PPPoA/PPPoE autosense on ATM VC with SNAP [6] encapsulation	12.1(1)DC	12.1(5)DC	12.2(2)B1
Remote Access into MPLS VPN	12.2(2)B	—	—
Routed bridge encapsulation (RBE)	12.0(5)DC	12.1(4)DC	12.2(2)B1
RBE Subinterface Grouping	12.1(4)DC	12.1(4)DC	12.2(2)B1
RBE unnumbered DHCP [7]	12.1(1)DC	12.1(4)DC	12.2(2)B1
RBE with DHCP	12.0(5)DC	12.1(4)DC	12.2(2)B1
RBE with DHCP Option 82	12.1(5)DC	12.1(5)DC	12.2(2)B1
RFC 1483 bridging	12.0(3)DC	12.1(4)DC	12.2(2)B1
RFC 1483 routing	12.0(3)DC	12.1(4)DC	12.2(2)B1
Aggregation and Virtual Private Networks (VPN)			
DHCP Relay Support for MPLS VPN Suboptions	12.2(4)B3	12.2(4)B3	12.2(4)B3
IP [8] Overlapping address pools (AOP)	12.1(5)DC	Not yet supported	Not yet supported
L2TP [9] Multi-Hop	12.1(1)DC	12.1(4)DC	12.2(2)B1
L2TP tunnel service authorization enhancement	12.1(1)DC	12.1(4)DC	12.2(2)B1
L2TP tunnel sharing	12.1(1)DC	12.1(4)DC	12.2(2)B1
L2TP tunnel switching [10]	12.1(1)DC	12.1(4)DC	12.2(2)B1
MPLS [11] Edge Label Switch Router (Edge LSR)	12.0(7)DC	Not yet supported	Not yet supported
MPLS Label Distribution Protocol	12.2(2)B	12.2(2)B	12.2(2)B1
MPLS Label Switch Controller (LSC) for BPX	12.0(7)DC	Not yet supported	Not yet supported
MPLS VPNs [12]	12.0(7)DC	12.2(2)B	12.2(2)B1
MPLS VPN ID	12.2(4)B3	12.2(4)B3	12.2(4)B3
PPPoA tunneled into L2TP	12.0(5)DC	12.1(4)DC	12.2(2)B1

Table 2 Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.2(4)B3 (continued)

Feature	NRP-1 Supported as of Cisco IOS Release	NRP-2 Supported as of Cisco IOS Release	NRP-2SV Supported as of Cisco IOS Release
PPPoE tunneled into L2TP	12.0(5)DC	12.1(4)DC	12.2(2)B1
Remote Access into MPLS VPN	12.1(5)DC	Not yet supported	Not yet supported
RFC 1577	12.0(3)DC	12.1(4)DC	12.2(2)B1
Session Limit per VRF	12.2(4)B3	12.2(4)B3	12.2(4)B3
VLAN [13] (ISL [14]) on NRP	12.0(3)DC	12.1(4)DC	12.2(2)B1
VLAN (802.1q) on NRP-2 GE[15]	Not applicable	12.1(5)DC	12.2(2)B1
Configuration and Monitoring			
ATM OAM Ping	12.2(4)B3	12.2(4)B3	12.2(4)B3
ATM PVC [16] Range Command	12.1(4)DC	12.1(4)DC	12.2(2)B1
Per VC error display	12.1(3)DC	12.1(5)DC	12.2(2)B1
Hardware Support			
ATM (OC-3, OC-12, DS3) Interfaces	12.0(3)DC	12.1(4)DC	12.2(2)B1
FE Interface: 10/100 auto-negotiation, auto-sensing	12.0(3)DC	Not applicable	Not applicable
GE Interface	Not applicable	12.1(5)DC	12.2(2)B1
Network Management Ethernet (NME)	12.0(5)DC	12.1(4)DC	12.2(2)B1
NRP 1+1 Redundancy	12.0(3)DC	Not yet supported	Not yet supported
IP and Routing			
Address Resolution Protocol (ARP)	12.0(3)DC	12.1(4)DC	12.2(2)B1
Border Gateway Protocol version 4 (BGP4)	12.0(3)DC	12.1(4)DC	12.2(2)B1
Enhanced Interior Gateway Routing Protocol (EIGRP)	12.0(3)DC	12.1(4)DC	12.2(2)B1
Generic routing encapsulation (GRE)	12.0(3)DC	12.1(4)DC	12.2(2)B1
Internet Group Management Protocol (IGMP)	12.0(3)DC	12.1(4)DC	12.2(2)B1
Internet Protocol (IP) forwarding	12.0(3)DC	12.1(4)DC	12.2(2)B1
IP multicast	12.0(3)DC	12.1(4)DC	12.2(2)B1
IP QoS—Policing, Marking, and Classification	12.2(2)B	12.2(2)B	12.2(2)B1
Intermediate System-to-Intermediate System (IS-IS)	12.0(3)DC	12.1(4)DC	12.2(2)B1
Network Address Translation (NAT) support for NetMeeting Directory	12.0(3)DC	12.1(4)DC	12.2(2)B1
NetFlow for RFC1483 into MPLS VPN	12.1(5)DC	Not yet supported	Not yet supported
Open Shortest Path First (OSPF)	12.0(3)DC	12.1(4)DC	12.2(2)B1
PIM [17] Dense Mode & Sparse Mode	12.0(3)DC	12.1(4)DC	12.2(2)B1
Routing Information Protocol (RIP)/RIP v2	12.0(3)DC	12.1(4)DC	12.2(2)B1
Transmission Control Protocol (TCP)	12.0(3)DC	12.1(4)DC	12.2(2)B1
Telnet	12.0(3)DC	12.1(4)DC	12.2(2)B1
Trivial File Transfer Protocol (TFTP)	12.0(3)DC	12.1(4)DC	12.2(2)B1

Table 2 Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.2(4)B3 (continued)

Feature	NRP-1 Supported as of Cisco IOS Release	NRP-2 Supported as of Cisco IOS Release	NRP-2SV Supported as of Cisco IOS Release
Transparent Bridging	12.0(3)DC	12.1(4)DC	12.2(2)B1
User Datagram Protocol (UDP)	12.0(3)DC	12.1(4)DC	12.2(2)B1
Web Cache Coordination Protocol (WCCP) version 1	12.0(3)DC	12.1(4)DC	12.2(2)B1
WCCP (v2)	12.0(7)DC	12.1(4)DC	12.2(2)B1
IP QoS			
IP QoS Dynamic Bandwidth Selection: IP policing/marking via CAR	12.2(2)B	12.2(2)B	12.2(2)B1
Network Management			
PPPoE Session Count MIB	12.2(2)B	12.2(2)B	12.2(2)B1
NRP: QoS			
Simple Network Management Protocol (SNMP) (v1, v2, and v3)	12.0(3)DC	12.1(4)DC	12.2(2)B1
SNMPv3 Proxy Forwarder	—	12.1(4)DC	12.2(2)B1
RADIUS/AAA			
Encrypted and Tagged VSA Support for RADIUS Attribute 91	12.2(4)B3	12.2(4)B3	12.2(4)B3
Enhancements to RADIUS VC Logging	12.2(4)B3	12.2(4)B3	12.2(4)B3
Extended support for RADIUS Attribute 32	12.2(4)B3	12.2(4)B3	12.2(4)B3
Framed Route VRF Aware	12.2(4)B3	12.2(4)B3	12.2(4)B3
Password Authentication Protocol (PAP)/Challenge Handshake Authentication Protocol (CHAP)	12.0(3)DC	12.1(4)DC	12.2(2)B1
Per VRF AAA	12.2(4)B3	12.2(4)B3	12.2(4)B3
Remote Authentication Dial-In User Service (RADIUS)	12.0(3)DC	12.1(4)DC	12.2(2)B1
RADIUS Attribute 8 (Framed-IP-Address) in Access Requests (IP Hint)	12.1(3)DC	12.1(4)DC	12.2(2)B1
RADIUS-based Session/Idle Timeout for LAC	12.2(4)B3	12.2(4)B3	12.2(4)B3
Support for RADIUS Attribute 77	12.2(4)B3	12.2(4)B3	12.2(4)B3
Support for RADIUS Attribute 52 and 53	12.2(4)B3	12.2(4)B3	12.2(4)B3
Terminal Access Controller Access Control System Plus (TACACS+) (admin login only)	12.0(3)DC	12.1(4)DC	12.2(2)B1
VPI [18]/VCI [19] RADIUS Request and RADIUS Accounting for PPPoA	12.0(3)DC	12.1(5)DC	12.2(2)B1
VPI/VCI in RADIUS Request and RADIUS Accounting for PPPoE	12.1(1)DC	12.1(5)DC	12.2(2)B1
Scalability and performance			
GRE Cisco express forwarding (CEF)	12.1(1)DC	12.1(5)DC	12.2(2)B1
LAC [20] CEF switching	12.1(3)DC	12.1(4)DC	12.2(2)B1

Table 2 Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.2(4)B3 (continued)

Feature	NRP-1 Supported as of Cisco IOS Release	NRP-2 Supported as of Cisco IOS Release	NRP-2SV Supported as of Cisco IOS Release
L2TP sessions per tunnel limiting	12.1(1)DC	12.1(4)DC	12.2(2)B1
NAT CEF switching	12.1(1)DC	12.1(4)DC	12.2(2)B1
Per VC buffer management	12.1(1)DC	12.1(4)DC	12.2(2)B1
PPPoA CEF	12.1(1)DC	12.1(4)DC	12.2(2)B1
PPPoE Fast Switching for Multicast	12.1(1)DC	12.1(5)DC	12.2(2)B1
RBE CEF switching	12.1(5)DC	12.1(5)DC	12.2(2)B1
Service Selection Gateway (NRP-SSG)			
PPP Aggregation Termination over Multiple Domains (PTA-MD)	12.0(3)DC	12.1(4)DC	12.2(2)B1
RADIUS Interim Accounting	12.0(5)DC	12.1(4)DC	12.2(2)B1
SSG AAA Server Group for Proxy RADIUS	12.2(2)B	12.2(2)B	12.2(2)B1
SSG Accounting Update Interval Per Service	12.2(4)B3	12.2(4)B3	12.2(4)B3
SSG AutoDomain	12.2(4)B3	12.2(4)B3	12.2(4)B3
SSG Autologoff	12.2(4)B3	12.2(4)B3	12.2(4)B3
SSG Autologon using Proxy RADIUS	12.2(4)B3	12.2(4)B3	12.2(4)B3
SSG Automatic Service Logon	12.0(3)DC	12.1(4)DC	12.2(2)B1
SSG CEF Switching	12.0(5)DC	12.1(4)DC	12.2(2)B1
SSG Default Network	12.0(3)DC	12.1(4)DC	12.2(2)B1
SSG DNS [21] Fault Tolerance	12.0(3)DC	12.1(4)DC	12.2(2)B1
SSG enable (default is disabled)	12.0(7)DC	12.1(4)DC	12.2(2)B1
SSG full username RADIUS attribute	12.1(3)DC	12.1(4)DC	12.2(2)B1
SSG Hierarchical Policing	12.2(4)B3	12.2(4)B3	12.2(4)B3
SSG Host Key	12.2(2)B	12.2(2)B	12.2(2)B1
SSG HTTP [22] Redirect (Phase 1)	12.1(5)DC	12.1(5)DC	12.2(2)B1
SSG Cisco IOS NAT support	12.0(5)DC	12.1(4)DC	12.2(2)B1
SSG Local Forwarding	12.1(1)DC	12.1(5)DC	12.2(2)B1
SSG Open Garden	12.2(2)B1	12.2(2)B1	12.2(2)B1
SSG Passthrough and Proxy Service	12.0(3)DC	12.1(4)DC	12.2(2)B1
SSG Prepaid Billing	12.2(4)B3	12.2(4)B3	12.2(4)B3
SSG Sequential and Concurrent Service	12.0(3)DC	12.1(4)DC	12.2(2)B1
SSG Service Defined Cookie	12.1(3)DC	12.1(4)DC	12.2(2)B1
SSG single host logon	12.1(3)DC	12.1(4)DC	12.2(2)B1
SSG Support for MAC Addresses in Accounting Records	12.2(4)B3	12.2(4)B3	12.2(4)B3
SSG TCP Redirect for Services (Phase 2)	12.2(4)B3	12.2(4)B3	12.2(4)B3
SSG with GRE	12.0(3)DC	12.1(5)DC	12.2(2)B1

Table 2 Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.2(4)B3 (continued)

Feature	NRP-1 Supported as of Cisco IOS Release	NRP-2 Supported as of Cisco IOS Release	NRP-2SV Supported as of Cisco IOS Release
SSG with Multicast	12.0(3)DC	12.1(4)DC	12.2(2)B1
SSG with L2TP Service Type	12.0(7)DC	12.1(4)DC	12.2(2)B1
TCP Redirect—Logon	12.1(5)DC	12.1(5)DC	12.2(2)B1
VPI/VCI Static binding to a Service Profile	12.0(5)DC	12.1(4)DC	12.2(2)B1
WebSelection	12.0(3)DC	12.1(4)DC	12.2(2)B1
Other Features and Feature Enhancements			
Segmentation and Reassembly Buffer Management Enhancements	12.1(1)DC	Not applicable	Not applicable
Session Scalability Enhancements	12.1(1)DC	12.1(4)DC	12.2(2)B1

1. VC = virtual circuit
2. PPP = Point-to-Point Protocol
3. IPCP = Internet Protocol Control Protocol
4. FE = Fast Ethernet
5. ATM = Asynchronous Transfer Mode
6. SNAP = Subnetwork Access Protocol
7. DHCP = Dynamic Host Configuration Protocol
8. IP = Internet Protocol
9. L2TP = Layer 2 Tunneling Protocol
10. 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 31.
11. MPLS = Multiprotocol Label Switching
12. VPN = Virtual Private Network
13. VLAN = Virtual LAN
14. ISL = Inter-Switch Link
15. GE = Gigabit Ethernet
16. PVC = permanent virtual circuit
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 12.2(4)B3. The table indicates the release in which each feature was originally introduced. All features supported in previous releases are included in Release 12.2(4)B3.

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. If you have a Cisco.com login account, you can find image and release information regarding features prior to Cisco IOS Release 12.2(4)B3 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 12.2(4)B3

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

Table 3 Features Supported by the Cisco 6400 NSP in Cisco IOS Release 12.2(4)B3 (continued)

Feature	Supported as of Cisco IOS Release
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
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
QoS	
ATM Policing by Service Category for SVC/SoftPVC	12.2(4)B3

Table 3 Features Supported by the Cisco 6400 NSP in Cisco IOS Release 12.2(4)B3 (continued)

Feature	Supported as of Cisco IOS Release
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
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 Cisco IOS Release 12.2(4)B3 and enhancements to existing features offered in prior releases.

New Hardware Features Supported in Release 12.2(4)B3

There are no new hardware features supported by the Cisco 6400 in Release 12.2(4)B3.

New Software Features Supported in Release 12.2(4)B3

This section lists the new software features supported by the Cisco 6400 in Release 12.2(4)B3.

ATM OAM Ping

The ATM OAM Ping feature modifies the **ping atm interface atm** and **ping (privileged)** commands, which can be used to send an Operation, Administration, and Maintenance (OAM) packet and display success when the response is received.

This feature provides two ATM OAM ping options:

- End loopback—Verifies end-to-end PVC integrity.
- Segment loopback—Verifies PVC integrity to the neighboring ATM device.

DHCP Relay Support for MPLS VPN Suboptions

The DHCP relay agent information option (option 82) enables a Dynamic Host Configuration Protocol (DHCP) relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement IP address or other parameter-assignment policies. The DHCP relay agent option is organized as a single DHCP option that contains one or more suboptions that convey information known by the relay agent.

In some environments, a relay agent resides in a network element that also has access to one or more MPLS Virtual Private Networks (VPNs). If a DHCP server wants to offer service to DHCP clients on those different VPNs, the DHCP server needs to know the VPN in which each client resides. The network element that contains the relay agent typically knows about the VPN association of the DHCP client and includes this information in the relay agent information option.

The DHCP relay agent forwards this necessary VPN-related information to the DHCP server using the following three suboptions of the DHCP relay agent information option:

- VPN identifier
- Subnet selection
- Server identifier override

The VPN identifier suboption is used by the relay agent to tell the DHCP server the VPN for every DHCP request it passes on to the DHCP server, and is also used to properly forward any DHCP reply that the DHCP server sends back to the relay agent.

The subnet selection option allows the separation of the subnet from the IP address used to communicate with the relay agent. In typical DHCP processing, the gateway address specifies both the subnet on which a DHCP client resides, as well as the IP address that the server can use to communicate with the relay agent. Situations exist where the relay agent needs to specify the subnet on which a DHCP client resides that is different from the IP address the server can use to communicate with the relay agent. The subnet selection suboption is included in the relay information option and passed on to the DHCP server. The gateway address is changed to the outgoing interface of the relay agent towards the DHCP server. The DHCP server uses this gateway address to send reply packets back to the relay agent.

The server identifier override suboption value is copied in the reply packet from the DHCP server instead of the normal server ID address. Using this information, the DHCP relay agent then sends the response back to the DHCP client on the correct VPN. The server identifier override suboption contains the incoming interface IP address, which is the IP address on the relay agent that is accessible from the client.

After adding these suboptions to the DHCP relay information option, the gateway address is changed to the outgoing interface of the relay agent towards the DHCP server. When the packets are returned from the DHCP server, the relay agent removes all options and forwards the packets to the DHCP client on the correct VPN.

Encrypted and Tagged VSA Support for RADIUS Attribute 91

This feature adds support for encrypted and tagged Cisco vendor-specific attribute (VSA) 91. Attribute 91 can be both encrypted and tagged.

The RADIUS attribute 91 feature allows you to specify a name (other than the default) of the tunnel terminator. By allowing the user to specify authentication names for the RADIUS server, attribute 91 supports the provision of compulsory tunneling in virtual private networks (VPNs). Also by specifying a name, you can establish a higher level of security when setting up VPN tunneling.

Once a network access server (NAS) has set up communication with a RADIUS server, you can enable a tunneling protocol. Some applications of tunneling protocols are voluntary, but others involve compulsory tunneling; that is, a tunnel is created without any action from the user and without allowing the user any choice in the matter. In those cases, new RADIUS attributes are needed to carry the tunneling information from the NAS to the RADIUS server to establish authentication. The new RADIUS attributes for attribute 91 are listed in Table 4.

Table 4 RADIUS Tunnel Attributes for Attribute 91

IETF RADIUS Tunnel Attribute	Equivalent TACACS+ Attribute	Supported Protocols	Description
Tunnel-Server-Auth-ID	gw-name	• Layer 2 Tunneling Protocol (L2TP)	Specifies the name used by the tunnel terminator (also known as L2TP network server or LNS) when authenticating tunnel setup with the tunnel initiator.

Note In compulsory tunneling, any security measures in place apply only to traffic between the tunnel endpoints. Encryption or integrity protection of tunneled traffic must not be considered as a replacement for end-to-end security.

Note Your RADIUS server must support tagged attributes to use RADIUS tunnel attribute 91.

The following section describes the specifics of an encrypted and tagged VSA.

Encrypted String and Tagged VSA

The encrypted string and tagged VSA is identical to the encrypted string VSA except for the addition of the Tag field before the Salt field. An encrypted string and tagged VSA must have the following field values:

- Type field must be 26 to specify a VSA.
- Vendor-ID field must be 9 to specify the Cisco vendor ID.
- Vendor Type field must be 36 to indicate an encrypted string VSA.

- Tag field is an 8-bit field that ranges from 0x01 through 0x1F, indicating the number of the tunnel that this attribute references. The system distinguishes the Tag field from the Salt field by the setting of the most significant (left most) bit—the Tag field sets this bit to 0, while the Salt field sets this bit to 1.
- Salt field is a two-byte field, and its most significant bit (left most) MUST be set to 1 to identify it as a Salt field and not a Tag field. The contents of each Salt field in a given Access-Accept packet must be unique to ensure the uniqueness of the encryption key that is used to encrypt the Attribute String.

The following illustrates the format of the encrypted string and tagged VSA:

```
 0               1               2               3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Type (26) |  Length       |           Vendor-Id (9)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont)          |Vendor type(36)| Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0   Tag      |1  Salt        | Salt(Cont)    | String ....
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Note See RFC 2865 for information about the RADIUS protocol. See RFC 2868 for information on the encryption/decryption algorithms used in RADIUS tunnel support.

Enhancements to DHCP Option 82 Support for RBE

The DHCP Option 82 Support for Routed Bridge Encapsulation (RBE) feature provides support for the DHCP relay agent information option when ATM routed bridge encapsulation is used.

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

This feature communicates information to the DHCP server using a suboption of the DHCP relay agent information option (option 82) called agent remote ID. The information sent in the Agent Remote ID includes an IP address identifying the relay agent and information about the ATM interface and the PVC over which the DHCP request came in. The DHCP server can use this information to make IP address assignments and security policy decisions.

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

Note The command “rbe nasip” has no effect on the Cisco 6400/NRP. It unconditionally returns the NSP NME IP Address. (See CSCdr40298.)

Service providers are increasingly using ATM routed bridge encapsulation to configure digital subscriber line (DSL) access. The DHCP Option 82 Support for Routed Bridge Encapsulation feature enables those service providers to use DHCP to assign IP addresses and DHCP option 82 to implement security and IP address assignment policies, such as limiting the number of IP addresses on specific ports or ATM VCs.

The enhancements to this feature are that for soft permanent virtual circuits (PVCs), as opposed to regular PVCs, the Cisco 6400, as the DHCP relay agent, uses the *egress* slot/subslot/port and VPI/VCI information in the Agent Remote ID.

For more information on this feature, refer to the "DHCP Option 82 Support for Routed Bridge Encapsulation" feature module at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ftrbeo82.htm

Enhancements to 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.

The enhancements on the Cisco 6400 are described in the note below.

Note When using soft permanent virtual circuits (PVCs), as opposed to regular PVCs, the Cisco 6400 returns the *egress* slot/subslot/port and VPI/VCI information. (See CSCdu64354, CScdr66199 and CSCdw30484).

For more information on this feature, refer to the "Miscellaneous Features" chapter of the *Cisco 6400 Feature Guide--Release 12.2(2)B* at the following URL:

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

Extended Support for RADIUS Attribute 32

The Extended Support for RADIUS Attribute 32 feature adds attribute 32 support from RADIUS Tunnel Attribute Extensions to IOS RADIUS. The network access server (NAS) is now identifiable to the RADIUS server, whether the NAS is a Cisco component or not.

Framed Route VRF Aware

The Framed-Route VRF Aware feature introduces support to make RADIUS Attribute 22 (Framed-Route) and a combination of Attribute 8 (Framed-IP-Address) and Attribute 9 (Framed-IP-Netmask) Virtual Routing Forwarding (VRF) aware. Thus, static IP routes can be applied to a particular VRF table rather than the global routing table.

MPLS VPN ID

Multiple VPNs can be configured in a router. You can use a VPN name (a unique ASCII string) to reference a specific VPN configured in the router. Alternately, you can use a VPN ID to identify a particular VPN in the router. The VPN ID follows a standard specification (RFC 2685). To ensure that the VPN has a consistent VPN ID, assign the same VPN ID to all the routers in the service provider network that services that VPN.

You can use several applications to manage VPNs by VPN ID. For more details on how server applications use the VPN ID, refer to the "Why Is a VPN ID Useful?" section.

Note Configuration of a VPN ID for a VPN is optional. You can still use a VPN name to identify configured VPNs in the router. The VPN name is not affected by the VPN ID configuration. These are two independent mechanisms to identify VPNs.

What Is a VRF?

For each VPN that is configured in a router, the router creates a Virtual Route Forwarding (VRF) instance. The VPN ID is stored in the corresponding VRF structure for the VPN.

The VRF table is a key element in the MPLS VPN technology. VRF tables exist on provider edge (PE) routers only. More than one VRF table can exist on a PE. A VPN can contain one or more VRF tables on a PE.

A VRF contains the routing information that defines the customer VPN site that is attached to a PE router. A VRF consists of the following elements:

- An IP routing table
- A derived Cisco Express Forwarding (CEF) table
- A set of interfaces that use the forwarding table
- A set of rules and routing protocols that determine what goes into the forwarding table

An IP routing table and the CEF table store packet forwarding information for each VRF. Another routing table and CEF table for each VRF prevent information from being forwarded outside a VPN and prevent packets that are outside a VPN from being forwarded to a router within the VPN.

Components of the VPN ID

Each VPN ID defined by RFC 2685 consists of the following elements:

- An Organizational Unique Identifier (OUI), a three-octet hex number.

  The IEEE Registration Authority assigns OUIs to any company that manufactures components under the ISO/IEC 8802 standard. The OUI is used to generate universal LAN MAC addresses and protocol identifiers for use in local and metropolitan area network applications. For example, an OUI for Cisco Systems is 00-03-6B (hex).
- A VPN index, a four-octet hex number, which identifies the VPN within the company.

Use the **vpn id** command and specify the VPN ID in the following format:

```
vpn id oui:vpn-index
```

A colon separates the OUI from the VPN index. See the **vpn id** command for more information.

Why Is a VPN ID Useful?

Remote access applications, such as the Remote Authentication Dial-In User Service (RADIUS) and Dynamic Host Configuration Protocol (DHCP), can use the MPLS VPN ID feature to identify a VPN. RADIUS can use the VPN ID to assign dial-in users to the proper VPN, based on the user authentication information.

DHCP

Using DHCP network administrators can centrally manage and automate the assignment of IP addresses in an organization's network. The DHCP application uses the VPN ID as follows:

1. A VPN DHCP client requests a connection to a PE router from a VRF interface.
2. The PE router determines the VPN ID associated with that interface.
3. The PE router sends a request with the VPN ID and other information for assigning an IP address to the DHCP server.
4. The DHCP server uses the VPN ID and IP address information to processes the request.
5. The DHCP server sends a response back to the PE router, allowing the VPN DHCP client access to the VPN.

Remote Authentication Dial-In User Service

A Remote Authentication Dial-In User Service (RADIUS) server (or daemon) provides authentication and accounting services to one or more client network-attached storage (NAS) devices. RADIUS servers authenticate users and return all configuration information necessary for the client to deliver service to the users.

Typically, a user login consists of a query (Access-Request) from the NAS to the RADIUS server and a corresponding response (Access-Accept or Access-Reject) from the server.

- The Access-Request packet contains the user name, encrypted password, NAS IP address, VPN ID, and port. The format of the request also provides information on the type of session that the user wants to initiate.
- The RADIUS server returns an Access-Accept response if it finds the user name and verifies the password. The response includes a list of attribute-value pairs that describe the parameters to be used for this session.

Per VRF AAA

Using the Per VRF AAA feature, Internet Service Providers (ISPs) can partition authentication, authorization, and accounting (AAA) services based on Virtual Route Forwarding (VRF). This permits the Virtual Home Gateway (VHG) to communicate directly with the customer RADIUS server associated with the customer VPN, without having to go through a RADIUS proxy. Thus, ISPs can scale their VPN offerings more efficiently because they no longer need to proxy AAA to provide their customers the flexibility demanded.

To support Per VRF AAA, AAA must be VRF aware. ISPs must define multiple instances of the same operational parameters—such as AAA server groups, method lists, system accounting, and protocol-specific parameters—and secure the parameters to the VRF partitions.

If an AAA configuration, such as a method list, is uniquely defined many times across the network access server (NAS), the specification of an AAA server that is based on IP addresses and port numbers may create an overlapping of private addresses between VRFs. Securing AAA method lists to a VRF can be accomplished from one or more of the following sources:

- Virtual Template—Used as a generic interface configuration.
- Service Provider AAA server—Used to associate a remote user with a specific VPN based on the domain name or Dialed Number Identification Service (DNIS). The server then provides the VPN-specific configuration for the virtual access interface, which includes the IP address and port number of the customer AAA server.
- Customer VPN AAA server—Used to authenticate the remote user and to provide user-specific configurations for the virtual access interface.

Note Global AAA accounting configurations and some AAA protocol-specific parameters cannot be logically grouped under the Virtual Template configuration.

AAA Server Configurations

To prevent possible overlapping of private addresses between VRFs, AAA servers must be defined in a single global pool that is to be used in the server groups. Servers can no longer be uniquely identified by IP addresses and port numbers.

Private servers (servers with private addresses within the default server group that contains all the servers) can be defined within the server group and remain hidden from other groups. The list of servers in server groups includes references to the hosts in the global configuration as well as the definitions of private servers.

Note If private server parameters are not specified, global configurations are used. If global configurations are not specified, default values are used.

All server operational parameters can be configured per host, per server group, or globally. Per-host configurations have precedence over per-server group configurations. Per-server group configurations have precedence over global configurations.

PPPoE over Ethernet (FE for NRP-1)

PPPoE over Ethernet enhances PPPoE functionality by adding direct connection to actual Ethernet and FastEthernet interfaces. PPPoE over Ethernet provides service-provider digital subscriber line (DSL) support by enabling multiple hosts on a shared Ethernet interface to open PPP sessions to multiple destinations with one or more bridging modems.

Note Note Fast switching is supported. PPPoE FIB switching will be supported for IP. All other protocols will be switched over process switching.

PPPoE over Ethernet with VLAN

PPPoE over Ethernet can be used with virtual LANs (VLANs).

For more information on PPPoE over Ethernet, refer to the "Configuring PPPoE over Ethernet" chapter in the "Configuring Broadband Access: PPP and Routed Bridge Encapsulation" section of the *Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fwan_c/wcfppp.htm#xtocid15

For more information on virtual LANs, refer to the routing and configuring routing VLAN documents in the *Cisco IOS Switching Services Configuration Guide, Release 12.2* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fswtch_c/swprt6/index.htm

PPPoE over Gigabit Ethernet (GE for NRP-2SV Only)

The PPPoE over Gigabit Ethernet feature enhances PPP over Ethernet (PPPoE) functionality by adding support for PPPoE and PPPoE over IEEE 802.1Q VLANs on Gigabit Ethernet interfaces. The PPPoE over Gigabit Ethernet feature is supported on Cisco 6400 chassis with Gigabit Ethernet line cards.

RADIUS-based Session/Idle Timeout for LAC

The RADIUS-based Session/Idle Timeout for L2TP Access Concentrator (LAC) feature enables the LAC to receive the session timeout from RADIUS via RADIUS Attribute 27 and an idle timeout within RADIUS Attribute 28 upon receiving a call directed via a specific L2TP tunnel to a certain Service Provider L2TP network server (LNS). The LAC should disconnect the session based on these timeouts.

A local configuration possibility of the idle timeout (session timeout is already implemented) would be desirable. In case both options are configured at the same time (a local configuration below the selected virtual template and session/idle timeout received via RADIUS), the values received via RADIUS must override the local configuration. All processing should happen via a Virtual Template mechanism. After the time of the idle or session timeout has expired, the LAC should send out a PADT towards the PPPoE client and the LNS to terminate the session.

Session Limit Per VRF

The Session Limit Per VPN Routing and Forwarding Instance (VRF) feature enables session limits to be applied on all VPDN groups associated with a common VPDN virtual template. Before the implementation of Session Limit Per VRF, a single default template carrying the configuration values of a subset of VPDN group commands were associated with all VPDN groups configured on the router. Session Limit Per VRF enables you to create, define and name multiple VPDN templates. You can then associate a specific template with a VPDN group. A session limit can be configured at the VPDN template level to specify a combined session limit for all VPDN groups associated with the configured VPDN template.

The benefit of the Session Limit Per VRF feature is that it controls the resources consumed by a single customer account by limiting the number of concurrent sessions terminating in a single VRF.

For more information on this feature, refer to the Session Limit Per VRF feature module at the following URL:

http://lbj.cisco.com/push_targets1/ucdit/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/12b_vrf.htm

Restrictions

Nesting of VPDN templates is not supported. A single VPDN group can only be associated with one template at a time.

SSG Accounting Update Interval Per Service

The Service Selection Gateway (SSG) Accounting Update Interval Per Service feature enhances SSG accounting by allowing users to configure an accounting interval for a particular service. Without the SSG Accounting Update Interval Per Service feature, all accounting information is sent simultaneously, and accounting information for a particular SSG service cannot be sent at a separate, independent interval.

SSG Accounting sends information such as billing, auditing, and reporting, so the SSG Accounting feature allows for more granular accounting interval options for all of these functions.

SSG Autodomain

When you configure SSG Autodomain, users can automatically connect to a service based on either Access Point Name (APN) or the domain part of the structured username specified in an Access-Request. When SSG Autodomain is configured, user authentication is not performed at the Network Access Server (NAS) AAA, but instead at the service (for example, at a AAA server within a corporate network).

Access Point Names

An APN identifies a Packet Data Network (PDN) that is configured on and accessible from a Gateway GPRS Support Node (GGSN). An access point is identified by its APN name. The Global System for Mobile Communication (GSM) standard 03.03 defines the following two parts of an APN:

- APN Network Identifier
- APN Operator Identifier

The APN Network Identifier is mandatory. The name of an access point in the form of an APN Network Identifier must correspond to the fully-qualified name in the Domain Name System (DNS) configuration for that network, and it must also match the name specified for the access point in the GGSN configuration. The GGSN also uniquely identifies an APN by an index number. The APN Operator Identifier is an optional name that consists of the fully-qualified DNS name, with the ending ".gprs."

The access points that are supported by the GGSN are preconfigured on the GGSN. When a user requests a connection in the GPRS network, the APN is included in the Create Packet Data Protocol (PDP) Request message. The Create PDP Request message is a GPRS Tunneling Protocol (GTP) message that establishes a connection between the Serving GPRS Support Node (SGSN) and the GGSN.

An APN has several attributes associated with its configuration that define how users can access the network at that entry point. For more information about configuring APNs, see the *APN Manager Application Programming Guide*.

SSG Autodomain

When using SSG Autodomain, you can automatically log in a user to a service based on either the APN or a structured username. Users can bypass the Service Selection Dashboard (SSD) and access a service, such as a corporate intranet.

SSG Autodomain makes it possible to log in a user to either Layer 2 Tunnel Protocol (L2TP) or proxy services. The username and password used to log in a user with Autodomain is the username and password provided by the user when logging into the General Packet Radio Service (GPRS) network. This password can be a dynamically generated password.

SSG Autodomain does not require SSG Vendor Specific Attributes (VSAs) when using a domain name as a means to determine which service to log in the user.

Autodomain uses a heuristic to determine the service into which the user is logged. When using Autodomain, the host object is not activated until successfully authenticated with the service. If the auto-service connection fails for any reason, the user login is rejected and an Access-Reject is returned to the Gateway GPRS Support Node (GGSN).

Autodomain service first checks for an APN (Called-Station-ID) and then for a structured username.

If Autodomain is enabled and the received Access-Request specifies an APN, then this APN is used for Autodomain selection unless it is a member of the APN Autodomain exclusion list. If an Autodomain is not selected based on APN, then the structured username is used. If a structured username is not supplied, or the supplied structured username is a member of the domain name exclusion list, then no Autodomain is selected and normal SSG user login proceeds. You can override these Autodomain selection defaults by configuring the **ssg auto-domain select** command. You can define the APN Autodomain exclusion list and the domain name exclusion list with the **ssg auto-domain exclude** command.

When Autodomain is enabled, an Autodomain profile is downloaded from the local AAA server. This profile is specified as an outbound service and the password is the globally configured service password.

You can configure SSG Autodomain in basic or extended mode. In basic mode, the Autodomain profile downloaded from the AAA server is a service profile. In extended Autodomain mode, the profile downloaded from the AAA server is a "virtual user" profile which contains one auto-service to an authenticated service such as a proxy or a tunnel. The "virtual user" profile defines the Autodomain

service. Connection to this auto-service occurs as it does for basic Autodomain, where the host object is not activated until the user is authenticated at the proxy or tunnel service. The presence of the SSD in extended Autodomain mode enables the user to access any other service in the specified user profile. If the "virtual user" profile does not have exactly one auto-service or the auto-service is not authenticated, the Autodomain login is rejected.

The Autodomain service profile can be a proxy or tunnel service. If the downloaded Autodomain service profile is a proxy service, the access-request is proxied to the appropriate domain AAA server. If the downloaded Autodomain service profile is a tunnel service, a PPP session is regenerated into an L2TP tunnel for the selected service. If no SSG-specific attributes are returned indicating the type of service required, the SSG uses a default set of attributes to regenerate the PPP session for the specified service.

SSG Autodomain attempts to log the user onto the remote service using the username and password specified in the original Access-Request. For structured user names, only the "user" part of the name is used unless the "X" attribute is present in the service profile. For VPDN-only type services (where no SSG attributes are present), it is not possible to specify use of the full structured username.

If you configure basic SSG Autodomain with a non authenticated service type such as passthrough, SSG rejects the login request because Autodomain bypasses user authentication at the local AAA server and requires that authentication be performed elsewhere.

SSG Autologoff

The SSG Autologoff feature enables the Cisco Service Selection Gateway (SSG) to verify connectivity with each host or user at configured intervals. If SSG detects that the connection has terminated, SSG will automatically initiate the logoff for that host or user.

When SSG autologoff is configured, the SSG will check the status of the connection with each host at configured intervals. If SSG finds that a host has been disconnected, SSG will automatically initiate the logoff of that host. SSG has two methods of checking the connectivity of hosts: ARP ping and ICMP ping.

ARP Ping

The Address Resolution Protocol (ARP) is an Internet protocol used to map IP addresses to MAC addresses in directly connected devices. A router that uses ARP will broadcast ARP requests for IP address information. When an IP address is successfully associated with a MAC address, the router stores the information in the ARP cache.

When SSG autologoff is configured to use ARP ping, SSG periodically checks the ARP cache tables. If a table entry for a host is found, SSG forces ARP to refresh the entry and checks the entry again after some configured interval. If a table entry is not found, SSG initiates autologoff for the host.

Note ARP ping should be used only in deployment scenarios where all hosts are directly connected.

Cisco recommends using ARP ping when possible because ARP entries are refreshed whenever there is network activity. In addition, ARP request packets are smaller than ICMP ping packets.

ICMP Ping

The Internet Control Message Protocol (ICMP) is a network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. An ICMP ping is the echo message and echo-reply message used to check for connectivity between devices.

When SSG autologoff is configured to use the ICMP ping mechanism, SSG invokes the callback function for successful pings or timeouts. In the case of timeout or ping error, the callback function checks the number of retries remaining and initiates ping again. If all the retries all used up, then SSG initiates logoff for the host. If the ping is successful, then SSG assumes the host has connectivity and no more attempts are made until the next ping interval.

ICMP ping will work in all types of deployment scenarios and supports overlapping IP users.

SSG AutoLogon Using Proxy RADIUS

Before the introduction of the SSG AutoLogon Using Proxy RADIUS feature, the SSG effectively acted as a RADIUS proxy for the Service Selection Dashboard (SSD). In this mode, when SSD needs to authenticate a user, it forwards an Access-Request to the SSG. The Access-Request uses the IP address and port number configured for RADIUS authentication on the SSG as well as the configured shared secret between the SSG and the SSD. When SSG receives a request from the SSD to authenticate a user, the SSG uses AAA to construct an Access-Request and send it to the AAA server. When SSG receives the Access-Accept, it processes it and forwards it to the SSD. In this implementation, SSG is far from acting as a generic RADIUS proxy and standard RADIUS protocol must be extended by the use of Vender Service Attributes (VSAs) to provide a control plane between the SSG and SSD. Without the VSA in the Access-Request, SSG did not function as a RADIUS proxy.

The SSG AutoLogon Using Proxy RADIUS feature enables the SSG to act as a RADIUS proxy for non-SSD clients whose Access-Requests do not contain VSAs. Non-SSD Access-Requests must originate from configured, trusted, downstream Network Access Server (NAS) IP addresses which share a RADIUS secret key with the SSG. This shared secret key is a different secret than the one shared between SSG and the SSD. You must configure the IP addresses for each router for which SSG is acting as a RADIUS proxy. Packets received from unrecognized sources are discarded.

When the SSG receives a valid Access-Request, it forwards it to the RADIUS server. The SSG performs a full, transparent proxy of the Access-Request to the RADIUS server, faithfully reproducing the attributes provided originally by the RADIUS client. If the Access-Request is successful, the AAA server responds with an Access-Accept and an SSG host object is created.

RADIUS Authentication and Authorization

A RADIUS client can be configured to use a RADIUS AAA server for user authentication. In a Cisco RADIUS client, the RADIUS server can be configured as a global AAA server for General Packet Radio System (GPRS) or individual servers per Access Point Name (APN). The RADIUS client sends an Access-Request to the AAA server to authenticate a user. The Access-Request contains attributes depending on whether the router is using CHAP or PAP.

After a successful authentication, the RADIUS AAA server responds to the Access-Request by sending an Access-Accept containing a RADIUS attribute.

The RADIUS attributes are part of the user database held on the RADIUS AAA server and can be modified or extended as required. You can configure the AAA server to select a user profile based on Called-Station-ID (Access Point Name [APN]) or Calling-Station-ID (MSISDN header field type for wireless clients using the Wireless Application Protocol [WAP]).

If the AAA is configured to select profiles based on Called-Station-ID, all users connecting to the same APN are given the same profile even though they have different assigned IP addresses.

The supplied username does not have to be unique for WAP users on the RADIUS client. These users are granted anonymous access and all have the same user name and password.

AAA authorization involves extracting all of the parameters needed to create the Packet Data Protocol (PDP) context. The authorization extracts the Framed-IP-Address and the Framed-IP-Netmask.

SSG Vendor-Specific Attributes

The SSG uses vendor-specific RADIUS attributes. If using the SSG with Cisco User Control Point (UCP) software, specify settings that allow processing of the SSG attributes while configuring the CiscoSecure Access Control Server (ACS) component. If using another AAA server, you must customize that server RADIUS dictionary to incorporate the SSG vendor-specific attributes.

SSG Hierarchical Policing

The Service Selection Gateway (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.

SSG allows subscribers to choose one or more types of services. Each type of service has its own bandwidth requirements (for instance, suppose an ISP has two types of services, regular and premium. The regular service is cheaper for customers but is allocated less bandwidth per customer than the premium service, which provides more bandwidth and a higher quality connection). SSG, therefore, requires a mechanism to insure bandwidth is distributed properly for customers using different types of services.

Traffic Policing is the concept of limiting the input or output transmission rate of traffic entering or leaving a node. In SSG, Traffic Policing can be used to allocate bandwidth between subscribers and between services to a subscriber to insure all types of services are allocated a proper amount of bandwidth. SSG uses per-user and per-user per-service policing to insure bandwidth is distributed properly between subscribers (per-user policing) and between services to a particular subscriber (per-user per-service policing). Because these policing techniques are hierarchical in nature (bandwidth can be first policed between users and then policed again between services to a particular user), this complete feature is called Hierarchical Policing for SSG.

Per-user policing is used to police the aggregated traffic destined to or sent from a particular subscriber and can only police the bandwidth allocated to a subscriber. Per-user policing cannot identify services to a particular subscriber and police bandwidth between these services.

Per-user per-service policing is used to police the types of services available to a subscriber. Per-user per-service policing is useful when an SSG subscriber is subscribed to more than one service and the multiple services are allocated different amounts of bandwidth (for instance, suppose a single subscriber is paying separately for Internet access and video service but is receiving both services from the same service provider. The video service would likely be allocated more bandwidth than the Internet access service and would likely cost more to the subscriber). Per-user per-service policing provides a mechanism for identifying the types of services (such as video or Internet access in the example) and allocating a proper amount of bandwidth to a particular service.

Hierarchical Policing for SSG Token Bucket Scheme

The Hierarchical Policing for SSG feature limits the input or output transmission rate of traffic based on a token bucket algorithm.

The token bucket algorithm used in SSG Hierarchical Policing analyzes a packet and determines whether the packet should be forwarded to its destination or dropped. The amount of available tokens in the token bucket determine whether a packet is forwarded or dropped; if enough tokens are available, the tokens are removed from the token bucket and the packet is forwarded. The packet is dropped if the token bucket does not have enough available tokens for the packet. Tokens are replenished in the token bucket at regular intervals.

SSG Prepaid Billing

The SSG Prepaid feature expands Service Selection Gateway (SSG) accounting features to allow service providers to offer prepaid billing for their services.

How SSG Prepaid Works

The SSG Prepaid feature allows SSG to determine whether to connect a subscriber to a service and for how long, based on how much credit a subscriber has. The credit, also called quota, is measured in either seconds for time or bytes for volume.

To obtain the quota for a connection, SSG submits an authorization request to the AAA server. The AAA server contacts the prepaid billing server which forwards the quota values to SSG. SSG then monitors the connection to track the quota usage. When the quota runs out, SSG performs reauthorization. During reauthorization, the billing server provides SSG with more quota if it is available; if the quota has run out, SSG logs the user off.

The following sections describe in more detail how authorization and reauthorization work:

- Service Authorization
- Service Reauthorization

Service Authorization

SSG differentiates prepaid services from postpaid services by the presence of a vendor specific attribute (VSA) called the Service Authorization VSA in the service profile. The presence of this attribute in the service profile means that SSG needs to perform authorization to get the quota values for the connection. Once a prepaid service has been identified, SSG generates an Access-Request called a Service Authorization Request.

In a mobile wireless scenario, where SSG is acting as a RADIUS proxy to the gateway GPRS support node (GGSN), the calling-station ID of the user is sent in the authorization request to the AAA server. In a non-RADIUS proxy environment where the access technology might not provide an MSISDN, SSG copies the value from the User-Name attribute into the Calling-Station-ID attribute field in the authorization request. The AAA server uses the Calling-Station-ID attribute in the Access-Request to perform authorization and return the quota parameters for that connection.

If a non-zero quota is returned, SSG creates a connection to the service with the initial quota value. The units for the quotas will be seconds for time and bytes for volume. A value of zero in a quota means the user has insufficient credit and is not authorized to use that service and the connection is not made. If the Quota attribute is not present in the authorization response, SSG will treat the connection as postpaid. However, if SSG receives an access reject or a quota of zero, SSG will not allow any further connection to that service.

Service Reauthorization

During the connection, if the quota is based on volume, SSG decrements the available quota until it runs out. If the quota is based on time, the connection is allowed to proceed for the quota duration. When the quota reaches zero, SSG issues a Service Reauthorization Request to the billing server. The Service Reauthorization Request includes a new SSG VSA called Quota Used.

If service reauthorization is unsuccessful, the billing server will respond to the Service Reauthorization Request with an Access-Accept containing a quota of zero. SSG will terminate the connection to the service at this point. If service reauthorization is successful, the billing server will return more quota to SSG and the connection will be allowed to continue.

SSG Support for MAC Addresses in Accounting Records

The SSG Support for MAC Addresses in Accounting Records feature allows Service Selection Gateway (SSG) to include the user's MAC address in RADIUS attribute 31 (Calling-Station-ID) in accounting records. The following restrictions apply to this feature:

- MAC address is available only in accounting records for users that are directly connected through Ethernet interfaces or bridged interfaces such as integrated routing and bridging (IRB) or routed bridge encapsulation (RBE) interfaces.
- MAC address will not be available in accounting records for users coming in on point-to-point interfaces, such as PPP users.
- MAC address will not be available for RADIUS proxy users. For RADIUS proxy users, RADIUS attribute 31 (Calling-Station-ID) in accounting records does not contain the MAC address but instead contains the MSISDN.

SSG TCP Redirect for Services (Phase 2)

A subscriber needs both user authentication and authentication for the services they are trying to access within the Service Selection Gateway (SSG). When both these conditions are not met, the request packet is discarded. Rather than dropping these packets, the SSG HTTP Redirect (Phase 1) feature allowed unauthenticated TCP traffic to be redirected to a default portal, such as SSD. The SSG TCP Redirect for Services (Phase 2) feature expands this capability to allow for an authenticated subscriber, who may not be authorized for a particular service, to be redirected to a list of captive portals.

The purpose of the Phase 2 feature is to implement redirection for services. After SSG authenticates a subscriber, the subscriber is offered a list of services that he is subscribed to. The subscriber may have to log in separately to these services based on the type of service. At this point, when the subscriber sends an upstream packet that has not been explicitly authorized by the service, the packet will be redirected to a list of captive portals for a set duration. The portal group can consist of one or more configured servers, arranged in the order in which they have been added.

Therefore, subscribers trying to access a TCP port on a network for a service to which they do not have access are redirected to one of the servers in the portal group. The subscribers' request packets coming in will be TCP-redirected in a round robin fashion. You can configure which portal group can be used as the destination for various packets, based on the packet destination address or the service that the subscriber is trying to access.

In addition, the default service redirect group redirects packets from a subscriber attempting to access a network for an unauthorized service that has not been defined by one of the service redirect groups. In this case, subscribers attempting to access an unauthorized location receive readable messages, as opposed to the current 404, page not found error message.

Similarly, SSG can be configured for TCP redirection to advertisement portals on a periodic fashion. And any SMTP traffic from an user can be redirected to a configured group of SMTP forwarding agents.

The format of the Cisco IOS CLI configuration commands in SSG TCP Redirect for Services Phase 2 is changed. The configuration commands have been grouped into one sub mode. Phase 2 CLI commands start with **ssg tcp-redirect** instead of **ssg http-redirect**.

Support for RADIUS Attributes 52 and 53

The RADIUS Attribute 52 and Attribute 53 feature introduces support for Attribute 52 (Acct-Input-Gigawords) and Attribute 53 (Acct-Output-Gigawords). Attribute 52 keeps track of the number of times the Acct-Input-Octets counter has rolled over the 32-bit integer throughout the course of the provided service; attribute 53 keeps track of the number of times the Acct-Output-Octets counter has rolled over the 32-bit integer throughout the delivery of service. Both attributes can be present only in Accounting-Request records where the Acct-Status-Type is set to "Stop" or "Interim-Update." These attributes can be used to keep accurate track of bill for usage.

Support for RADIUS Attribute 77

The RADIUS Attribute 77 feature introduces support for Attribute 77 (Connect-Info) to carry the textual name of the virtual circuit class associated with the given permanent virtual circuit (PVC). (Although attribute 77 does not carry the unspecified bit rate (UBR), the UBR can be inferred from the class name used if one UBR is set up on each class.) Attribute 77 is sent from the network access server (NAS) to the RADIUS server via Accounting-Request and Accounting-Response packets.

New Hardware Features Supported in Release 12.2(2)B5

There are no new hardware features supported by the Cisco 6400 in Release 12.2(2)B5.

New Software Features Supported in Release 12.2(2)B5

There are no new software features supported by the Cisco 6400 in Release 12.2(2)B5.

New Hardware Features Supported in Release 12.2(2)B4

There are no new hardware features supported by the Cisco 6400 in Release 12.2(2)B4.

New Software Features Supported in Release 12.2(2)B4

There are no new software features supported by the Cisco 6400 in Release 12.2(2)B4.

New Hardware Features Supported in Release 12.2(2)B3

There are no new hardware features supported by the Cisco 6400 in Release 12.2(2)B3.

New Software Features Supported in Release 12.2(2)B3

There are no new software features supported by the Cisco 6400 in Release 12.2(2)B3.

New Hardware Features Supported in Release 12.2(2)B2

There are no new hardware features supported by the Cisco 6400 in Release 12.2(2)B2.

New Software Features Supported in Release 12.2(2)B2

There are no new software features supported by the Cisco 6400 in Release 12.2(2)B2.

Limitations and Restrictions

- The number of sessions and tunnels supported for the NRP-2 and NRP-2SV modules in Cisco IOS Release 12.2(4)B3 has changed to support of 6000 sessions per 2000 tunnels. See Table 6 and Table 7 for more information.
- L2TP Multihop by remote tunnel hostname is not supported in Cisco IOS Release 12.2(4)B3.

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

  Enter the **lcp renegotiation always** configuration command on the L2TP network server (LNS) vpdn-group.
- The traffic shaping feature is not supported for the NRP-2 module only.

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2(4)B3 that can apply to the Cisco 6400.

Upgrading from Cisco IOS Release 12.2(2)B to Cisco IOS Release 12.2(4)B3

If you currently have a Cisco 6400 broadband aggregator running Cisco IOS Release 12.2(2)B, and you are upgrading to Cisco IOS Release 12.2(4)B3, please note the configuration differences detailed in Table 5.

Table 5 Differences Between CIsco IOS Release 12.2(2)B and Cisco IOS Release 12.2(4)B3

Cisco IOS Release 12.2(2)B	Cisco IOS Release 12.2(4)B3
Cisco Express Forwarding (CEF) Configuration Support	
You must enable CEF before Service Selection Gateway (SSG) can be enabled.	You must enable CEF on the router before you can enable SSG functionality. If CEF is not enabled and you attempt to configure SSG, the following error message is displayed: SSG : Please enable ip cef first You can enable CEF in global configuration mode using the following command: Router(config)# **ip cef** However, if required, you can disable CEF at the individual interface level without affecting SSG.
Data Packet Forwarding	
When a data packet is received from a user, SSG checks in the default network and open garden networks. If the check fails, the packet is checked and forwarded to the connected services of the user.	When a data packet is received from a user, SSG attempts to forward the packet by doing a longest match in the connected services of the user. If the packet is not destined for the connected services, SSG attempts to forward the packet to the configured default network or open garden networks. If the user is connected to an Internet service, SSG checks if the destination IP address of the packet falls in the default network or open garden networks. If so, the packet is forwarded to the respective destination; otherwise, the packet is forwarded to the Internet service.
Data Packet Processing Overhead	
When SSG is enabled, there is an extra packet processing overhead for packets from non-SSG interfaces. Every packet from a non-SSG interface is intercepted and minimally processed by SSG. This introduces an extra latency for packets from non-SSG interfaces.	There is no extra packet processing latency for packets from non-SSG configured interfaces. Only packets from configured SSG interfaces are intercepted and processed by SSG.
DNS Packet Processing in Open Garden Configuration	
Domain Name System (DNS) domain lookup is done first in the domains configured in the open garden services. If a match is not found, then DNS domain lookup is done in the connected services of the user.	DNS domain lookup is done first in the connected services of the user. If a match is not found, then DNS domain lookup is done in the domains configured in the open garden services.
DNS Packet Accounting	
DNS packets from a client are not accounted in the host or connection. This may cause erroneous accounting statistics at the host or connection level.	DNS packets are treated and accounted as any other data packets.
Host Timestamp Update	
The timestamp in the host object is updated only when a packet from the client is forwarded to a connected service. If a host is accessing the Cisco Subscriber Edge Services Manager (SESM) and an idle timeout is configured, the host may get logged off.	The timestamp is updated for any packet from the client, preventing an erroneous logoff. The only exception is if the packet is destined for the SSG router itself, in which case the timestamp is not updated.

Table 5 Differences Between Clsco IOS Release 12.2(2)B and Cisco IOS Release 12.2(4)B3 (continued)

Cisco IOS Release 12.2(2)B	Cisco IOS Release 12.2(4)B3
L2TP Tunnel Support	
The **aaa new-model** command is not required to configure SSG to establish L2TP tunnels.	SSG uses a new application program interface (API) to support API tunnel-type services. You must use the following commands in global configuration mode to configure SSG to establish L2TP tunnels: Router(config)# **aaa new-model** Router(config)# **vpdn-enable**
Multiple Service Binding	
Only one service can be bound to a single interface or subinterface. If multiple services are bound to a single interface and a user connects to these services, the packets are not accounted correctly in the per-connection statistics maintained by SSG.	Multiple services can be bound to a single interface or subinterface without affecting connection accounting.
RADIUS Authentication for PPP Users	
User authentication is attempted by SSG using RADIUS protocol. To configure SSG to intercept user PPP authentication requests, you must configure PPP authentication. You do not need to specify RADIUS as the authentication protocol. Router(config)# **aaa authentication ppp default local** Router(config)# **aaa authorization network default group radius** In the preceding configuration, SSG still sends an authentication request to the RADIUS server for a PPP user, even though a local authentication is specified in the CLI.	User authentication is done by Cisco IOS PPP leveraging AAA RADIUS protocol for authenticating all PPP users. Using 12.2(2)B configuration, PPP will attempt to find the user configuration on the router itself and fail. You must issue the following command in global configuration mode for authentication to be attempted: Router(config)# **aaa authentication ppp default group radius**
Replaced command: debug http-redirect	
The **debug ssg http-redirect** command is available.	The **debug ssg http-redirect** command is not available and has been replaced by the **debug ssg tcp-redirect** *options* command to debug issues related to redirection.
Virtual Route-Forwarding (VRF) Support for GRE tunnels	
SSG does not leverage Cisco IOS CEF and does not create CEF tables.	SSG leverages Cisco IOS CEF for data forwarding. This necessitates the use of CEF tables for data path switching. SSG creates and maintains a CEF table on each service (uplink) interface or subinterface. This is a VRF scalability issue, whereby the number of CEF tables that SSG can create and support is limited by VRF scalability on a given platform or NRP card. For example, if GRE tunnels are configured on the service side, SSG attempts to create a CEF table per GRE tunnel, which, due to memory resource limitation on the router, may prevent SSG from creating CEF tables.

Session and Tunnel Scalability

Table 6 shows the number of sessions and tunnels supported for the NRP modules in Cisco IOS Release 12.2(4)B3. While using NRP-SSG, Cisco IOS Release 12.2(4)B3 supports the number of sessions and tunnels shown in Table 7.

Table 6 Session and Tunnel Scalability in Cisco IOS Release 12.2(4)B3

	NRP-1		NRP-2 and NRP-2SV	
Protocol	**Supported Sessions**	**Supported Tunnels**	**Supported Sessions**	**Supported Tunnels**
L2TP PPPoA	up to 1700	up to 300	up to 6000	up to 2000
L2TP PPPoE	up to 2000	up to 300	up to 6000	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 Auto	up to 2000	—	up to 8000	—
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
Multilink PPP	up to 1100	—	up to 1254	

I

Table 7 NRP-SSG Session and Tunnel Scalability in Cisco IOS Release 12.2(4)B3

	NRP-1		NRP-2 and NRP-2SV	
Protocol with NRP-SSG	**Supported Sessions**	**Supported Tunnels**	**Supported Sessions**	**Supported Tunnels**
L2TP PPPoA	up to 1000	up to 100	up to 4000	up to 2000
L2TP PPPoE	up to 1000	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 1800	up to 75	up to 8000	up to 1700

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.

NRP-2SV Scalability Tuning Parameters

Following are scalability tuning parameter values used during testing for 6000 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
```

Tip With PPPoA over L2TP network architecture, a few PPP sessions may not have IP addresses allocated during system reboot or interface flapping. If you encounter this problem, configure ppp ncp timeout in the template on LNS as shown here:

```
interface Virtual-Template1
ppp timeout ncp 60
```

It is important to note a potential negative impact on PPPoX termination scenarios:

The default is no time-out at all. Configuring **ppp timeout ncp 60** tells the router if NCP cannot be established within 60 seconds to tear down LCP and start all over again.

Note that you should only configure **ppp timeout ncp 60** if you encounter the IP address allocation problem described here. Do not configure the timeout indiscriminately or to any local termination PPPoA/PPPoE deployment.

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.

NRP-1 Scalability Tuning Parameters

This section describes the scalability tuning parameters that should be used for running large numbers of sessions on the NRP-1.

```
interface ATM0/0/0
 hold-queue 1000 in
 hold-queue 1000 out
!
interface Virtual-Template1
 keepalive 120
 ppp max-configure 255
 ppp timeout retry 15
 ppp timeout authentication 15
```

Field Notices and Bulletins

- Field Notices—Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/770/index.shtml. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/770/index.shtml.
- Product Bulletins—If you have an account on Cisco.com, you can find product bulletins at http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml. If you do not have a Cisco.com login account, you can find product bulletins at http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml.
- *What's Hot for IOS Releases: Cisco IOS Release 12.2(4)B3—What's Hot for IOS Releases: Cisco IOS Release 12.2(4)B3* provides information about caveats that are related to deferred software images for Cisco IOS Release 12.2(4)B3. If you have an account on Cisco.com, you can access *What's Hot for IOS Releases: Cisco IOS Release 12.2(4)B3* at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml or by logging in and selecting **Software Center: Cisco IOS Software: What's Hot for IOS Releases: Cisco IOS Release 12.2(4)B3**.
- *What's New for IOS — What's New for IOS* lists recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. If you have an account on Cisco.com, you can access *What's New for IOS* at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml or by logging in and selecting **Software Center: Cisco IOS Software: What's New for IOS**.

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(4)T1 are also in Cisco IOS Release 12.2(4)B3.

For information on caveats in Cisco IOS Release 12.2(4)T1, 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(4)B3 is in synchronization with Cisco IOS Release 12.2(4)T1.

Caveat numbers and brief descriptions are listed in the tables in this section. For details about a particular caveat, go to Bug Toolkit at:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl

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 44.

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(4)B3

All the caveats listed in Table 8 are open in Cisco IOS Release 12.2(4)B3 for the Cisco 6400 NRP-1, NRP-2, NRP-2SV, and NSP. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 8 Open Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B3

Product	Caveat ID Number	Description
All	CSCin03269	CEF table creation takes long time when 2000 GRE tunnels configured
	CSCdv72965	Crash due to watchdog @ parse_radius_response
	CSCdx24528	PPP Packet redirected to same interface in endless loop
NRP-1	CSCdr50376	Some sessions drop when the VCs are oversubscribed
	CSCdr82324	L2TP:VPDN:Releasing idb for LAC/LNS tunnel
	CSCdw65741	Incorrect tag rewrite for default route in VRF
	CSCdx05811	show atm pvc VPI#/VCI# does not show any output
	CSCdx12542	NRP1 FE with ISL encapsulation is causing FCS errors on WS-X5225R
NRP-2, NRP-2SV	CSCin07477	MPLS:Control comm. between bpx-atm switch and nrp2 stopped
	CSCdr52399	NRP2 reset during image download breaks NSP
	CSCdr55905	config write code doesnt check for free space on disk

Table 8 Open Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B3 (continued)

Product	Caveat ID Number	Description
	CSCdr70852	With service compress-config enabled, NRP2 does not comp saved conf
	CSCdr76980	NSP disk1 operation affect NRP2 from loading image from disk0
	CSCdt57785	NRP2:Can not see startup config context if confreg set to 0x**4*
	CSCdt92169	boot -n boot option does not properly drop into gdb with pam console
	CSCdu58024	NRP2 GE<->GE back to back with no auto nego,not able to recover link
	CSCdu66436	False Counter throughput Statistics
	CSCdv32871	NRP2:Cut and paste a range pvc config produces a trace back message
	CSCdw23646	Traceback for shaping with policing
	CSCdw38947	RP2:ISIS Routing updates not send with AAL5NLPID,SNAP,MUX in GE-ATM
	CSCdw54113	Malloc failures with traffic for 8K PPPoE sessions while QoS on
NSP	CSCdp76911	Rptd NRP rebts w/another NRP in ROMMON may cause NSP PVC NO HW RSRCS
	CSCdr71571	disk access error after NRP2 crashes with config file open
	CSCdr87109	Traceback messages during boot w/ hw-mod shutdown in config
	CSCdw25976	Cutover alarm not generated after NRP1 switchover
	CSCdx17417	Input errors coun on NSP ATM 0/0/0 virtual interface

Table 9 lists open caveats that pertain to MIB files for the Cisco 6400 for Release 12.2(4)B3.

Table 9 Open Caveats for Cisco 6400 MIBs for Release 12.2(4)B3

Product	Caveat ID Number	Description
MIBs	CSCdw67048	ciscoDslProvisionMIB takes too long to timeout

Closed and Resolved Caveats—Release 12.2(4)B3

All the caveats listed in Table 10 are closed or resolved in Cisco IOS Release 12.2(4)B3 for the Cisco 6400 NRP-1, NRP-2, NRP-2SV, and the NSP. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 10 Closed or Resolved Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B3

Product	Caveat ID Number	Description
All	CSCdw75532	7400(MC-MLPPP):LNS crash with MALLOC FAIL while bringing sessions
	CSCdx24528	PPP Packet redirected to same interface in endless loop
NRP-1, NRP-2, NRP-2SV	CSCdv29433	Router crash when setany command are sent to it
	CSCdv73314	6400 sent out two access requests when no L2TP
	CSCdv74128	LNS with 12.2(5.7)T lcp is renegotiated wo/ lcp renegotiation cfgd
	CSCdw02017	EVENT-MIB set action requires rw string in mteEventSetContextName

Table 10 Closed or Resolved Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B3 (continued)

Product	Caveat ID Number	Description
NRP-1	CSCdm92848	EHSA minor alarm pop up after 2 non-redundancy NRP boot up
	CSCdp05523	NAT:Large address range & portlist chains cause cpu spikes
	CSCdp59354	Egress traffic to RBE ints process sw w/ FE+ISL & <<bridge irb>>
	CSCdr04534	PPPoA/L2TP:2000 sess, some connected routes are not est after flap
	CSCdt74755	NAT cause high CPU utilization
	CSCdu01557	NRP crashes with BADFREEMAGIC message
	CSCdu09764	c6400:NRP crash w/ bad magic on allocated block
	CSCdu56256	Fast ethernet interface reports %AMDP2_FE-3-UNDERFLO, trnsmit error
	CSCdu64354	Option 82 and Radius VPI/VCI authentication does not work with S-PVC
	CSCdv63811	Memory corruption in I/O pool
	CSCdv74851	NRP1 with IRB crashes with bus error
	CSCdv82697	NRP1:IRB Routing protocol updates not working with ISIS
	CSCdw59637	With oam enabled, atm subinterface up/down after reload
	CSCdw66951	Tunneluser not able to ping service if ping packet size > tunnel MTU
	CSCdw73249	SAR Not Setting up VC when VC Line Protocol is Down
	CSCdw75186	LAC forwards all new calls to tunnel not reachable but not yet shut
	CSCdw81924	Port CSCdm89718 to NRP1 (code currenlty only on 7200 & rsp)
NRP-2, NRP-2SV	CSCdr70852	With service compress-config enabled, NRP2 does not comp saved conf
	CSCdr76980	NSP disk1 operation affect NRP2 from loading image from disk0
	CSCdr83804	ROMMON: NRP2 crashes if NSPs disk0 is removed during NRP2 idnld
	CSCdr95295	NRP2:total memory size displayed is incorrect
	CSCdu69223	buffer leak in PAM MBOX
	CSCdv55811	NRP2 crashed @se64_close_rx_vc_desc when trying to change vc encap
	CSCdv75114	NRP2:ISIS routing updates not sent with AAL5NLPID, SNAP, MUX in GE-ATM
	CSCdw13019	Loss of IP/SNMP connectivity to NRP2 when NSP has large run-conf
	CSCdw30583	Loss of IP connectivity between NSP and NRP2 with big config files
	CSCdw32965	NRP2 crash when traffic switched over from another NRP2
	CSCdw37740	Heavy loading cause NSP cant ping atm OAM to NRP2
	CSCdw60122	OAM CRC10 Errored packets can cause an input queue wedge on ATM0/0/0
	CSCdw60560	Malloc failure for I/O memory during bursty traffic
	CSCdx07784	port CSCdw67214 to NRP2(ISL fails with packets > 1484)
NSP	CSCdt33730	Port scans caused ALIGN-3-READEXCEPTION on NSP
	CSCdv35547	%SCHED-3-THRASHING error w/ traceback on NSP
SSG	CSCdw13690	NRP crashes while scaling PPPoA sessions over GRE tunnels
	CSCdw49074	NRP2 Crashes while scaling 8k PPPoA Sessions over 2k GRE tunnels

Table 10 Closed or Resolved Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B3 (continued)

Product	Caveat ID Number	Description
	CSCdw54156	NRP SSG L2TP/PPPoX tunnel sessions drops with traffic
	CSCdw79480	SSG PPPoX/L2TP: Not able to Scale 4000Host over 2000 Service
	CSCdx06795	NRP2 SSG PPPoX/L2TP tunnel sessions drop with traffic GE-ATM path

Table 11 lists resolved caveats that pertain to MIB files for the Cisco 6400 for Release 12.2(4)B3.

Table 11 Closed or Resolved Caveats for Cisco 6400 MIBs for Release 12.2(4)B3

Product	Caveat ID Number	Description
Mibs	CSCdu89655	OLD-CISCO-CHASSIS-MIB Object chassisId.0 write error
	CSCdv18939	ifXEntry returns null for objects like ifHCInOctets and ifHCOutOctet
	CSCdv77631	SNMP returns incorrect values for sysObjetID, cardType, chassisType
	CSCdv83898	atmIntfCurrentlyOAMFailingPVcls.1 causing SNMP-3-CPUHOG
	CSCdw13019	Loss of IP/SNMP connectivity to NRP2 when NSP has large run-conf
	CSCdw52894	NRP crashes while walking the cdslVcClassTable
	CSCdw71419	ciscoFlashFileTable is looping while doing a SNMP walk
	CSCdw80181	watchdog timer expired
	CSCdw85034	Memory leak in CISCO-DSL-PROVISION-MIB
	CSCdw86632	Getnext returns uninstatiated objects in the CISCO-ATM2-MIB

Open Caveats—Release 12.2(2)B5

No severity 1 or severity 2 open caveats exist for Cisco IOS Release 12.2(2)B5 for the Cisco 6400 NRP-2, Cisco 6400 NRP-2SV, Cisco 6400 NRP-1, and the Cisco 6400 NSP. For information about any open caveats in Cisco IOS Release 12.2(4) T1, see the *Caveats for Cisco IOS Release 12.2 T*, which is located on Cisco.com and the Documentation CD-ROM.

Closed or Resolved Caveats—Release 12.2(2)B5

All the caveats listed in Table 12 are closed or resolved in Cisco IOS Release 12.2(2)B5 for the Cisco 6400 NRP-2, Cisco 6400 NRP-2SV, Cisco 6400 NRP-1, and the Cisco 6400 NSP.

Table 12 Closed or Resolved Caveats for Cisco 6400 NRP and Cisco 6400 NSP for Release 12.2(2)B5

Product	Caveat ID Number	Description
NRP-2 and NRP-2SV	CSCdw60560	Malloc failure for I/O memory during bursty traffic
NRP-1 and NSP	CSCdw52894	NRP crashes while walking the cdslVcClassTable
	CSCdw68465	NRP1: memory corruption in vpdn session failure recording

Table 12 Closed or Resolved Caveats for Cisco 6400 NRP and Cisco 6400 NSP for Release 12.2(2)B5 (continued)

Product	Caveat ID Number	Description
NRP-2, NRP-2SV, NRP-1, and NSP	CSCdv66216	EE48:ST:RP crashed while trying remove 48 VPNs from 48 DS3 interface
	CSCdv83883	Spurious memory while doing walking snmp tree
	CSCdw80181	watchdog timer expired
	CSCdw85034	Memory leak in CISCO-DSL-PROVISION-MIB

Open Caveats—Release 12.2(2)B4

No severity 1 or severity 2 open caveats exist for Cisco IOS Release 12.2(2)B4 for the Cisco 6400 NRP-2, Cisco 6400 NRP-2SV, Cisco 6400 NRP-1, and the Cisco 6400 NSP. For information about any open caveats in Cisco IOS Release 12.2(4) T1, see the *Caveats for Cisco IOS Release 12.2 T*, which is located on Cisco.com and the Documentation CD-ROM.

Closed or Resolved Caveats—Release 12.2(2)B4

All the caveats listed in Table 13 are closed or resolved in Cisco IOS Release 12.2(2)B4 for the Cisco 6400 NRP-2, Cisco 6400 NRP-2SV, Cisco 6400 NRP-1, and the Cisco 6400 NSP.

Table 13 Closed or Resolved Caveats for Cisco 6400 NRP and Cisco 6400 NSP for Release 12.2(2)B4

Product	Caveat ID Number	Description
NRP-2 and NRP-2SV	CSCdw60122	OAM CRC10 Errored packets can cause an input queue wedge on ATM0/0/0
	CSCdw83085	Need to enhance ATM driver debugging
NRP-1 and NSP	CSCdv74851	NRP1 with IRB crashes with bus error
	CSCdw05710	6400:pvc goes inactive, %ATMCES-1-ERRCREATEVC
	CSCdw81924	Port CSCdm89718 to NRP1 (code currently only on 7200 & rsp)
NRP-2, NRP-2SV, NRP-1, and NSP	CSCdw42849	PPPoE session is not cleared
	CSCdw65903	An error can occur with management protocol processing. Please use the following URL for further information: http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

Open Caveats—Release 12.2(2)B3

All the caveats listed in Table 14 are open in Cisco IOS Release 12.2(2)B3 for the Cisco 6400 NRP-2 and NRP-2SV.

Table 14 Open Caveats for Cisco 6400 NRP-2 and NRP-2SV for Release 12.2(2)B3

Product	Caveat ID Number	Description
NRP-2 and NRP-2SV	CSCdw13019	Loss of IP/SNMP connectivity to NRP2 when NSP has large run-conf
	CSCdw26218	Virtual-access gets stuck in LCP closed state
	CSCdw30583	Loss of IP connectivity between NSP and NRP2 with big config files
	CSCdw32965	NRP2 crash when traffic switched over from another NRP2
	CSCdw37740	Heavy loading cause NSP cant ping atm OAM to NRP2

Closed or Resolved Caveats—Release 12.2(2)B3

All the caveats listed in Table 15 are closed or resolved in Cisco IOS Release 12.2(2)B3 for the Cisco 6400 NRP-2 and NRP-2SV.

Table 15 Closed or Resolved Caveats for Cisco 6400 NRP-2 and NRP-2SV for Release 12.2(2)B3

Product	Caveat ID Number	Description
NRP-2 and NRP-2SV	CSCdu29467	ipfast_frag.c:possible dereference null pointer
	CSCdw11239	PE of MPLS-VPN stops forward pkts after stress with large pktsizes
	CSCdw37282	Traffic does not pass when reset occurs with Traffic shaping enabled

Open Caveats—Release 12.2(2)B2

All the caveats listed in Table 16 are open in Cisco IOS Release 12.2(2)B2 for the Cisco 6400 NRP-1, NRP-2, and NRP-2SV. All the caveats listed in Table 17 are open in Cisco IOS Release 12.2(2)B2 for the Cisco 6400 NSP. These tables list only severity 1 and 2 caveats and select severity 3 caveats. Table 18 lists caveats that pertain to MIB files for the Cisco 6400 for Release 12.2(2)B2.

Table 16 Open Caveats for Cisco 6400 NRP for Release 12.2(2)B2

Product	Caveat ID Number	Description
NRP-2	CSCdr95295	NRP2:total memory size displayed is incorrect
	CSCdt57785	NRP2:Can not see startup config context if confreg set to 0x**4*
	CSCdu58024	NRP2 GE<->GE back to back with no auto nego, not able to recover link
	CSCdu58091	Copy file from NRP2 to NSP causes NSP Bus Error exception
	CSCdu66436	False Counter throughput Statistics
	CSCdv32871	NRP2:Cut and paste a range pvc config produces a trace back message
	CSCdv39868	Assertion failed error on console during debugs
	CSCdv55745	Err msg NULL RX particle header when trying to change encap type
	CSCdv55811	NRP2 crashed @se64_close_rx_vc_desc when trying to change vc encap
	CSCdv56280	GE:Auto-nego CLI command is missing
	CSCdv70703	NRP2:After removing the multicast boundary mroute table not updated
	CSCdv75114	NRP2:ISIS routing updates not sent with AAL5NLPID, SNAP, MUX in GE-ATM
	CSCdv77023	NRP2:Multicast client does not respond to ICMP packet with CEF ON
	CSCdw07107	Loss of IP/SNMP connectivity to NRP2 when NSP has large run-conf
NRP-1	CSCdp05523	NAT:Large address range & portlist chains cause cpu spikes
	CSCdp59354	Egress traffic to RBE ints process sw w/ FE+ISL & <<bridge irb>>
	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
	CSCdt74755	NAT cause high CPU utilization
	CSCdu01557	NRP crashes with BADFREEMAGIC message
	CSCdu09764	c6400:NRP crash w/ bad magic on allocated block
	CSCdu56256	Fast ethernet interface reports %AMDP2_FE-3-UNDERFLO, trnsmit error
	CSCdu64354	Option 82 and RADIUS VPI/VCI authentication does not work with S-PVC
	CSCdv19996	FE interface on some NRP1 boards drops packets
	CSCdv63811	Memory corruption in I/O pool
	CSCdv74851	NRP1 with IRB crashes with bus error
	CSCdv75177	NRP1-PPPoA- Poor traffic performances caused by ATM0/0/0 drops
	CSCdv82697	NRP1:IRB Routing protocol updates not working with ISIS
SSG	CSCdv05136	SSG Service Profile Name should be legally formatted

Table 17 Open Caveats for Cisco 6400 NSP for Release 12.2(2)B2

Product	Caveat ID Number	Description
NSP	CSCdr71571	Disk access error after NRP2 crashes with config file open
	CSCdt33730	Port scans caused ALIGN-3-READEXCEPTION on NSP
	CSCdt39132	Unable to sync files/dir if the path+filename is more than 53 chars
	CSCdt41423	Secondary hangs when transitioning to primary on failover
	CSCdu23253	ATM i/f with NRP is not properly displaying alarm state
	CSCdv35547	%SCHED-3-THRASHING error w/ traceback on NSP

Table 18 Open Caveats for Cisco 6400 MIBs for Release 12.2(2)B2

Product	Caveat ID Number	Description
MIBs	CSCdv82930	Threshold Value for cPppoeVcSessionThresholdTrap not defaulting
	CSCdv83898	atmIntfCurrentlyOAMFailingPVcls.1 causing SNMP-3-CPUHOG
	CSCdv83902	SNMP timeouts walking ciscoPppoeMIB
	CSCdv86358	System reset when activate CISCO-FTP-CLINET-MIB cfcRequestTable row

Closed and Resolved Caveats—Release 12.2(2)B2

All the caveats listed in Table 19 are closed or resolved in Cisco IOS Release 12.2(2)B2 for the Cisco 6400 NRP-1 and NRP-2. All the caveats listed in Table 20 are closed or resolved in Cisco IOS Release 12.2(2)B2 for the Cisco 6400 NSP. These tables list only severity 1 and 2 caveats and select severity 3 caveats.

Table 19 Closed or Resolved Caveats for Cisco 6400 NRP for Release 12.2(2)B2

Product	Caveat ID Number	Description
NRP-2 and NRP-1	CSCdt84904	DHCP offer forwarded out all mpls vpn cable subinterfaces
	CSCdw00126	Input queue wedged on BV1

Table 19 Closed or Resolved Caveats for Cisco 6400 NRP for Release 12.2(2)B2 (continued)

Product	Caveat ID Number	Description
NRP-2	CSCdm92848	EHSA minor alarm pop up after 2 non-redundancy NRP boot up
	CSCdr88742	wr mem on NRP2 doesnt generate a warning/error mess when no disk0
	CSCdr98773	Create subinterfaces & pvcs doesnt show on config file
	CSCds26319	VA interfaces counters show 3X the actual counts when client is NRP2
	CSCds47327	NRP2_SE64-3-ULD_BADVC message when shut atm sub-interface
	CSCds79849	CPUHOG while clearing counters w/large number of PPP sessions
	CSCds83542	Spurious Memory access during PPPOA/L2TP session bringup
	CSCds83689	NRP2: some session may not come up after interface flap in L2TP
	CSCdt15119	NRP2:ISIS routing updates are not sent with AAL5NLPID,SNAP,MUX encap
	CSCdt19637	CPU hog when doing clear counters
	CSCdt37234	ATM0/0/0 stops passing traffic on the NRP2 in 12.1(4.4)DC1
	CSCdt51547	Packet drop with ip verify unicast reverse-path
	CSCdt51810	Crash at nrp_ip2_tag_feature in 12.1(5)DC throttle
	CSCdt65960	Access-list not working on VTY when we telnet GigEth port
NRP-1	CSCdv47420	NRP1 ethernet interface does not get dynamic ip address
	CSCdv51304	Option 82 not removed from unnumbered DHCP responses
	CSCdv57549	NRP1 FE Interface going to reset state
SSG	CSCdt73695	SSG HTTP-Redirection Feature is not working for RBE User
	CSCdt76953	Memory leaks in Net Background processes when logon to ssg l2tp

Table 20 Closed or Resolved Caveats for Cisco 6400 NSP for Release 12.2(2)B2

Product	Caveat ID Number	Description
NSP	CSCdr65451	ILMI does NOT come up on DS3 interface
	CSCdr88742	wr mem on NRP2 dont generate a warning/error mess when no disk0
	CSCds51415	PAM mailbox Config not valid on NRP1 while booting
	CSCdt29127	ILMI failure on atm0/0/0 after NSP switchover
	CSCdt45629	Problem with VC resource allocation
	CSCdt46373	Rwait never cleaned up--problem with VC management?
	CSCdt47730	OSPF and XtagATM interface issues on NRP when NSP reloads
	CSCdt65698	NSP switch over cause NRP2 in certain slot to reset
	CSCdt71049	APS unidirectional switches bidirectionally
	CSCdt71080	APS force switch to non-operational protect should not be allowed
	CSCdt76617	PVCs on NSP sub-interface stops passing traffic after reload

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 T 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 T: Release Notes

  On the Documentation CD-ROM at:

  Cisco IOS Software Configuration: Cisco IOS Release 12.2 T: 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 "Software Caveats" 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 Carrier-Class Broadband Aggregator

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

Aggregation Solutions: Cisco 6400 Carrier-Class Broadband Aggregator

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 21 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 21 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

Table 21 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *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
• *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

Table 21 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *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
• *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 43.