Release Notes for Cisco 6400 Carrier-Class Broadband Aggregator for Cisco IOS Release 12.2(4)B7

November 2002

Cisco IOS Release 12.2(4)B7

OL-2951-03

These release notes for the Cisco 6400 Carrier-Class Broadband Aggregator describe the enhancements provided in Cisco IOS Release 12.2(4)B7.

For a list of the software caveats that apply to Cisco IOS Release 12.2(4)B7, see the "Software Caveats" section on page 33, and *Caveats for Cisco IOS Release 12.2T*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Contents

These release notes describe the following topics:

CISCO SYSTEMS

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

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(4)B7 and includes the following sections:

Memory Recommendations

Table 1 lists the memory recommendations for the Cisco 6400 aggregator.

Table 1   Memory Recommendations for the Cisco 6400 Aggregator

Product Name	Software Module Description	Image Name	Recommended Minimum DRAM Memory	Recommended Minimum Flash Memory
NRP	Boot image	c6400r-boot-mz	—	—
NRP-2 and NRP-2SV	IOS NRP-2 base IOS NRP-2 mutlidomain IOS NRP-2 web selection	c6400r2sp-g4p5-mz	256 MB for up to 6500 sessions. 512 MB for over 6500 sessions.	—
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 if you are upgrading 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. If you have more sessions, the requirement is 512-MB DRAM.

Note When you are 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. If you have more sessions, you need 128-MB DRAM. If you are using the NRP-1, for an upgrade from an earlier release to Cisco IOS Release 12.2(4)B7, 128-MB DRAM is recommended.

Supported Hardware

Cisco IOS Release 12.2(4)B7 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 if you want 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)B7 works with the Cisco Service Selection Dashboard (SSD) Releases 2.5(1) and 3.0(1), and Subscriber Edge Services Manager (SESM) Release 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)B7
```

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)B7
```

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 aggregator, including upgrading a single or dual-NRP system to a new software release, see the *Cisco 6400 Software Setup Guide*. For general information about upgrading to a new software release, see the product bulletin *Cisco IOS Upgrade Ordering Instructions*.

Feature Set Tables

The Cisco IOS software is packaged in software images. Each image contains a 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 Table 2 might not be cumulative or list all of the features in each image. 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 57.

Table 2   Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.2(4)B7

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 (VPNs)			
DHCP Relay Support for MPLS VPN Suboptions	12.2(4)B3	12.2(4)B3	12.2(4)B3
IP Overlapping Address Pools (OAP)	12.1(5)DC	Not yet supported	Not yet supported

Table 2   Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.2(4)B7 (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[8] 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[9]	12.1(1)DC	12.1(4)DC	12.2(2)B1
MPLS[10] 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[11]	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
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[12] (ISL[13]) on NRP	12.0(3)DC	12.1(4)DC	12.2(2)B1
VLAN (802.1q) on NRP-2 GE[14]	—	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[15] 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	—	—
GE Interface	—	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

Table 2   Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.2(4)B7 (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
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[16] Dense Mode and 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
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			
Dynamic Subscriber Bandwidth Selection (ATM VC for Layer 2 QoS)	—	—	12.2(4)B3
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

Table 2   Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.2(4)B7 (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
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 Attributes 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[17]/VCI[18] 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[19] CEF Switching	12.1(3)DC	12.1(4)DC	12.2(2)B1
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 Auto Logoff	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[20] 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

Table 2   Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.2(4)B7 (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 Host Key	12.2(2)B	12.2(2)B	12.2(2)B1
SSG HTTP[21] 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
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	—	—
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. L2TP = Layer 2 Tunneling Protocol.

9. In Cisco IOS Release 12.1(5)DC, L2TP tunnel switching for the NRP-2 was tested and is supported at the same session and tunnel levels as the NRP-1. For more information, see Table 6 on page 30.

10. MPLS = Multiprotocol Label Switching.

11. VPN = Virtual Private Network.

12. VLAN = Virtual LAN.

13. ISL = Inter-Switch Link.

14. GE = Gigabit Ethernet.

15. PVC = permanent virtual circuit.

16. PIM = Protocol Independent Multicast.

17. VPI = virtual path identifier.

18. VCI = virtual channel identifier.

19. LAC = L2TP Access Concentrator.

20. DNS = Domain Name System.

21. 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)B7. 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)B7.

> **Note** Table 3 might not be cumulative or list all of the features in each image. For a list of the T-train features in this platform, refer to Feature Navigator. For more information about Feature Navigator, see the

Table 3   Features Supported by the Cisco 6400 NSP in Cisco IOS Release 12.2(4)B7

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)	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.371 and 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

Table 3   *Features Supported by the Cisco 6400 NSP in Cisco IOS Release 12.2(4)B7 (continued)*

Feature	Supported as of Cisco IOS Release
ATM Traffic Classes	
Available Bit Rate (ABR) (EFCI[1] + RR[2]) + Minimum Cell Rate (MCR)	12.0(4)DB
Constant Bit Rate (CBR)	12.0(4)DB
Per-VC or per-VP CBR Traffic Shaping	12.0(4)DB
Shaped CBR VP Tunnels (up to 128)	12.0(4)DB
Substitution of Other Service Categories in Shaped VP Tunnels	12.0(4)DB
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 (VBR-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)DISK
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

Table 3   *Features Supported by the Cisco 6400 NSP in Cisco IOS Release 12.2(4)B7 (continued)*

Feature	Supported as of Cisco IOS Release
Web Console	12.0(4)DB
QoS	
ATM Policing by Service Category for SVC/Soft PVC	12.2(4)B3
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 or Changed Information

This section describes features available in Cisco IOS Release 12.2(4)B7 and enhancements to existing features offered in earlier releases.

There are no new hardware or software features supported by the Cisco 6400 aggregator in Cisco IOS Releases:

- 12.2(2)B7
- 12.2(2)B6
- 12.2(2)B5
- 12.2(2)B4
- 12.2(2)B3
- 12.2(2)B2

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 to 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 it forwards 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 that the relay agent passes on to the DHCP server. It is also used for the proper forwarding of 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 and the IP address that the server can use to communicate with the relay agent. Situations exist where the relay agent needs to specify a subnet on which a DHCP client resides that is different from the IP address that the server can use to communicate with the relay agent. The subnet selection suboption is included in the relay information option and is passed on to the DHCP server. The gateway address is changed to the outgoing interface of the relay agent used by 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 of the relay agent that is accessible from the client.

After adding these suboptions to the DHCP relay information option, the DHCP server changes the gateway address to the outgoing interface of the relay agent used by 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.

Dynamic Subscriber Bandwidth Selection (ATM VC for Layer 2 QoS)

The Dynamic Subscriber Bandwidth Selection (DBS) feature is available for the NRP-2SV only. This feature enables wholesale service providers to sell different classes of service to retail service providers by controlling bandwidth at the ATM virtual circuit (VC) level. ATM Quality of Service (QoS) parameters from the subscriber domain are applied to the ATM PVC on which a PPPoE or PPPoA session is established.

Using DBS you can set the ATM permanent virtual circuit (PVC) traffic-shaping parameters to be dynamically changed based on the RADIUS profile of a PPP over Ethernet (PPPoE) or PPP over ATM (PPPoA) user logging in on the PVC. If the user is the first user on that PVC, the RADIUS profile values override the default values of the PVC. If users already exist on the PVC, the new value overrides the existing configuration only if it is higher than the existing value. If multiple PPPoE sessions are allowed on a subscriber VC, the highest peak cell rate (PCR) and sustainable cell rate (SCR) of all of the sessions are selected as the PCR and SCR of the VC.

Traffic-shaping parameters can be configured locally by IOS CLI in VC-mode, VC-class, range mode, or PVC-in-range mode. These parameters have a lower priority and are overridden by the shaping parameters specified in the domain service profile. Traffic-shaping parameters that are CLI configured at the VC class interface or subinterface level are treated as the default QoS parameters for the PVCs to which they apply. These parameters are overridden by the domain service profile QoS parameters of the domain the user is logged in to. If no VC class is configured, the default is the unspecified bit rate (UBR).

When a network access server (NAS) sends a domain authorization request and receives an affirmative response from the RADIUS server, this response may include a "QoS-management" string via vendor-specific attribute 26 for QoS management in the NAS. The QoS management values are configured as part of the domain service profile attributes on the RADIUS server. These values contain PCR and SCR values for particular PVCs. If the QoS specified for a domain cannot be applied on the PVC that the session belongs to, the session is not established.

Changing PVC traffic parameters because of new simultaneous PPPoE sessions on the PVC does not cause existing PPPoE sessions that are already established to disconnect. Changing domain service profile QoS parameters on the RADIUS server does not cause traffic parameters to automatically change for PVCs that have existing sessions.

When you enter the **dbs enable** or **no dbs enable** command to configure or unconfigure DBS, existing sessions are not disconnected. If you have a session that has been configured for DBS and you enter the **no dbs enable** command on a VC, additional sessions that are configured will display DBS configured QoS values until the first new session is up. After the first session is brought up, the VC has default and locally configured values. If you configure the **dbs enable** command after multiple sessions are already up on the VC, all sessions on that VC have DBS QoS parameters.

Encrypted and Tagged VSA Support for RADIUS Attribute 91

The Encrypted and Tagged VSA Support for RADIUS Attribute 91 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. It thus 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 you are setting up VPN tunneling.

Once a 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 attribute for attribute 91 are listed in Table 4.

Table 4   RADIUS Tunnel Attributes for Attribute 91

IETF RADIUS Tunnel Attribute	Equivalent TACACS+ Attribute	Supported Protocol	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.

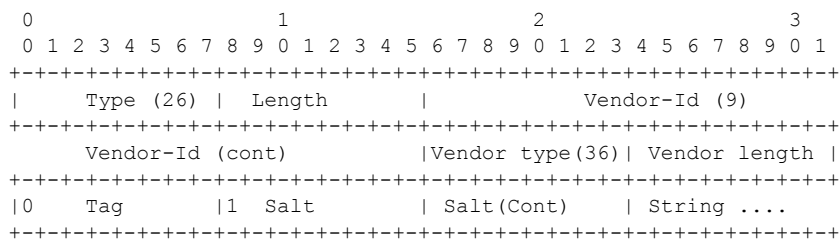**Note**   Your RADIUS server must support tagged attributes in order for you to use RADIUS tunnel attribute 91.

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, 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 (leftmost) bit; this bit is 0 in the Tag field or 1 in the Salt field.
- Salt field is a 2-byte field, and its most significant bit (leftmost) *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. This ensures 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 it forwards 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 Cisco 6400 NSP.

Note The command **rbe nasip** has no effect on the Cisco 6400 NRP. The 6400 unconditionally returns the NSP NME IP address.

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

As an enhancement to this feature, for soft permanent virtual circuits (PVCs), the Cisco 6400—functioning 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.

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

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 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 Virtual Route Forwarding support for RADIUS Attribute 22 (Framed-Route), Attribute 8 (Framed-IP-Address), and Attribute 9 (Framed-IP-Netmask). With this feature, static IP routes can be applied to a particular VRF table rather than to 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. Alternatively, 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 of 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 "Using a VPN ID" 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 for identifying VPNs.

VRF Definition

For each VPN that is configured in a router, the router creates a Virtual Route Forwarding instance. The VRF instance contains the routing information that defines the customer VPN site that is attached to a provider edge (PE) router. A VRF instance 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.

VPN ID Components

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 4-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
```

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

Using a VPN ID

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 to the PE router, allowing the VPN DHCP client access to the VPN.

RADIUS

A RADIUS server (or daemon) provides authentication and accounting services to one or more client 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 about the type of session that the user wants to initiate. For example, if the query is presented in character mode, the inference is "Service-Type = Exec-User," but if the request is presented in PPP packet mode, the inference is "Service Type = Framed User" and "Framed Type = PPP."

- 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 associate the parameters with the VRF partitions.

If an AAA configuration, such as a method list, is uniquely defined many times across the NAS, the specification of an AAA server that is based on IP addresses and port numbers might create an overlapping of private addresses between VRF configurations. Associating AAA method lists with VRF partitions 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 of 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   Fast switching is supported. PPPoE forwarding information base (FIB) switching is supported for IP. All other protocols are 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 *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 aggregator chassis that have 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 Attribute 27 and the idle timeout from RADIUS Attribute 28. The LAC should disconnect the session based on these timeouts.

If you have configured the idle timeout locally below the selected virtual template, and the LAC receives a session/idle timeout through RADIUS, the values received through RADIUS must override the local configuration. 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 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 was 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. You can configure a session limit 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://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122b/122b_4/12b_vrf.htm

VPDN Restrictions

Nesting of VPDN templates is not supported. A single VPDN group can be associated with only 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 interval for reporting of accounting information. Without this feature, all accounting information is sent simultaneously. With the SSG Accounting Update Interval per Service feature, accounting information for a particular SSG service can be sent at separate, independent intervals.

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 NAS AAA. Instead it is performed at the server for the service (for example, at an AAA server within a corporate network).

Access Point Names

An Access Point Name (APN) identifies a Packet Data Network (PDN) that is configured on and accessible from a Gateway General Packet Radio Service (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 are the username and password provided by the user when the user logs in to the GPRS network. This password can be dynamically generated.

SSG Autodomain does not require SSG vendor-specific attributes (VSAs) when using a domain name as a means to log a user in to a particular service.

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 GGSN.

Autodomain service 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 using 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 for 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 on to the remote service using the username and password specified in the original Access-Request. For structured usernames, 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), you cannot specify use of the full structured username.

If you configure basic SSG Autodomain with a nonauthenticated 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 automatically initiates the logoff for that host or user.

When SSG autologoff is configured, the SSG checks the status of the connection with each host at configured intervals. If SSG finds that a host has been disconnected, SSG automatically initiates 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 broadcasts 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** Use ARP ping only in deployment scenarios where all hosts are directly connected.

We recommend 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 consists of the echo message and the 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 of the retries are used up, SSG initiates logoff for the host. If the ping is successful, SSG makes no more ping attempts until the next ping interval.

ICMP ping works 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 does 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 NAS IP addresses that 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. Using a Cisco RADIUS client, you can configure the RADIUS server as a global AAA server for 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 Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (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 (Mobile Station ISDN [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 username 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 you are using the SSG with Cisco User Control Point (UCP) software, specify settings that allow processing of the SSG attributes. You can specify these setting when you configure the CiscoSecure Access Control Server (ACS) component. If you are 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. SSG, therefore, requires a mechanism for ensuring that bandwidth is distributed properly for customers using different types of services.

Traffic policing is the concept of limiting the rate at which traffic enters or leaves a node. In SSG, Traffic policing can be used to allocate bandwidth between subscribers and between services to a subscriber to ensure that all types of services are allocated a proper amount of bandwidth. SSG uses per-user and per-user per-service policing to ensure 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 SSG Hierarchical Policing.

Per-user policing is used to police the aggregated traffic destined for or sent from a particular subscriber. You can use it to police the bandwidth allocated to a subscriber. Per-user policing cannot identify services to a particular subscriber and it therefore cannot allocate 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 subscribes to more than one service and the multiple services are allocated different amounts of bandwidth. Per-user per-service policing provides a mechanism for identifying the types of services (such as video or Internet access) and allocating a proper amount of bandwidth to each 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. If the token bucket does not have enough tokens available for the packet, the packet is dropped. Tokens are replenished in the token bucket at regular intervals.

SSG Prepaid Billing

The SSG Prepaid feature expands SSG accounting features to allow service providers to offer prepaid billing for their services.

SSG Prepaid Process

The SSG Prepaid feature allows SSG to use a subscriber's credit allotment to determine whether to connect the subscriber to a service and for how long. 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

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 are 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 treats the connection as postpaid. However, if SSG receives an access reject or a quota of zero, SSG does 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 responds to the Service Reauthorization Request with an Access-Accept that contains a quota of zero. SSG terminates the connection to the service at this point. If service reauthorization is successful, the billing server returns more quota to SSG and the connection is allowed to continue.

SSG Support for MAC Addresses in Accounting Records

The SSG Support for MAC Addresses in Accounting Records feature allows 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:

- A 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.

- A MAC address is not available in accounting records for users coming in on point-to-point interfaces, such as PPP users.

- A MAC address is not available for RADIUS proxy users. For RADIUS proxy users, RADIUS attribute 31 (Calling-Station-ID) in accounting records contains the MSISDN rather than the MAC address.

SSG TCP Redirect for Services—Phase 2

Subscribers need both user authentication and authentication for the services they are trying to access within the SSG. If 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 might 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 or she is subscribed to. The subscriber might have to log in separately to these services depending 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 is 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 are 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 a 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 a standard "404, page not found" error message.

Similarly, SSG can be configured for TCP redirection to advertisement portals on a periodic basis. Any SMTP traffic from a 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 submode. Phase 2 CLI commands start with **ssg tcp-redirect** instead of **ssg http-redirect**.

Support for RADIUS Attributes 52 and 53

The RADIUS Attributes 52 and 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 NAS to the RADIUS server in Accounting-Request and Accounting-Response packets.

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 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)B7. L2TP Multihop by domain is supported in Cisco IOS Release 12.2(4)B7 by entering the **lcp renegotiation always** command on the L2TP network server (LNS) vpdn-group.

- When you flap an ATM subinterface that has traffic shaping enabled, the NRP-2SV SAR can fail. If this occurs, all sessions will eventually timeout and disconnect. This issue can also occur when you change vc-class parameters. If you use traffic shaping and you need to change configurations related to virtual circuits with traffic shaping configured, you must shutdown the ATM main interface, make your configurations changes, then bring up the ATM main interface.

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2(4)B7 that can apply to the Cisco 6400 aggregator.

Upgrading from Cisco IOS Release 12.2(2)B to Cisco IOS Release 12.2(4)B7

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)B7, note the differences detailed in Table 5.

Table 5   Differences Between CIsco IOS Release 12.2(2)B and Cisco IOS Release 12.2(4)B7

Cisco IOS Release 12.2(2)B	Cisco IOS Release 12.2(4)B7
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 correct 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.

Table 5   Differences Between Clsco IOS Release 12.2(2)B and Cisco IOS Release 12.2(4)B7 (continued)

Cisco IOS Release 12.2(2)B	Cisco IOS Release 12.2(4)B7
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.	The timestamp is updated for any packet from the client, preventing an erroneous logoff. The only exception occurs if the packet is destined for the SSG router itself, in which case the timestamp is not updated.
L2TP Tunnel Support	
You do not need the **aaa new-model** command 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 statistical accuracy.
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 sequence, 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 the AAA RADIUS protocol for authenticating all PPP users. Using Release 12.2(2)B configuration, PPP attempts to find the user configuration on the router itself and fails. 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. You can use the command to debug issues related to redirection.

Table 5   Differences Between Cisco IOS Release 12.2(2)B and Cisco IOS Release 12.2(4)B7 (continued)

Cisco IOS Release 12.2(2)B	Cisco IOS Release 12.2(4)B7
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—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 for each GRE tunnel, which, due to memory resource limitations on the router, might 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)B7. If you are using the NRP-SSG, Cisco IOS Release 12.2(4)B7 supports the number of sessions and tunnels shown in Table 7.

Table 6   Session and Tunnel Scalability in Cisco IOS Release 12.2(4)B7

	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	—

Table 7   NRP-SSG Session and Tunnel Scalability in Cisco IOS Release 12.2(4)B7

Protocol with NRP-SSG	NRP-1		NRP-2 and NRP-2SV	
	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 occurring. (8K/2K L2TP sessions/tunnels don't come up even after a long wait.)

```
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 might 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
```

There is 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.

Configure **ppp timeout ncp 60** only 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 prevents the issuing of 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—You can view Cisco 6400 aggregator-specific field notices at http://www.cisco.com/en/US/products/hw/routers/ps314/prod_field_notices_list.html. You can view 12.2B field notices at http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_field_notices_list.html

- Product Bulletins—You can view Cisco 6400 aggregator-specific product bulletins at http://www.cisco.com/en/US/products/hw/routers/ps314/prod_bulletins_list.html. You can view 12.2B product bulletins at http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_field_notices_list.html

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)B7.

For information on caveats in Cisco IOS Release 12.2(4)T1, see *Caveats for Cisco IOS Release 12.2T*, which lists severity 1 and 2 caveats and select severity 3 caveats.

Caveat numbers and brief descriptions are listed in the tables in this section. For details about a particular caveat, go to the Bug Navigator located at http://www.cisco.com/support/bugtools/. 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 57.

Open Caveats—Release 12.2(4)B7

All of the caveats listed in Table 8 are open in Cisco IOS Release 12.2(4)B7 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)B7

Product	Caveat ID Number	Title	Description	Workaround
All	CSCdx91120	%SYS-2_WATCHDOG: Process = PPPOE background daemon.	If a permanent virtual circuit (PVC) that is configured for PPPoX autosensing is removed, the router is sometimes reloaded due to watchdog timeout.	Determine the virtual access (VA) interface for each of the PPPoE sessions and enter **clear interface virtual-interfacexxx.** When all of the sessions on the virtual circuit are gone, the virtual circuit can be removed.
	CSCdz31478	AAA Acct Proc traceback on shut interface	Under atm0/0/0, there are 4 multipoint subinterfaces with 400 PPPoA sessions each, but no traffic flowing. AAA accounting network default start-stop group radius is configured.	None.
NSP	CSCdy07600	NSP Reload when formatting slot 0	When trying to format an ATA card, the **format slot 0** command can cause the NSP to reload and failover to the redundant NSP prior to the format completing.	Do not use the **format slot** command on the NSP. Use **format disk** instead.

Table 8 **Open Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B7 (continued)**

Product	Caveat ID Number	Title	Description	Workaround
NRP-1	CSCdx93277	Idle timer not working correctly in 12.2(2)BX1.	On a Cisco 6400 NRP1 terminating PPPoE sessions in a PPP Termination and Aggregation (PTA) setup, the idle timer that is downloaded from the RADIUS server on the Virtual-Access interfaces associated to the PPPoE user sessions might not work correctly.	None.
	CSCdz22008	Buffer leak in PAM mbox	PAM mbox is a mechanism for NRP and NSP to communicate. There are special I/O buffers allocated for PAM mbox. These I/O buffers decrease and eventually become exhausted. When this happens, communications cease between NRP and NSP.	None.
NRP-2	CSCdu58024	NRP-2 GE<->GE back to back with no auto nego, not able to recover link.	GE interfaces of the NPR2 are connected back to back with auto negotiation turned off. Initially the connectivity works fine. However, when one of the GE ports is toggled using **no shut** and **shut**, the connectivity breaks. With auto negotiation off, the connections is not broken.	None.
	CSCdy02662	SAR chip run out of transmit buffer link pointers.	This problem occurs only with frequent changes to the shaper value defined in vc-class. The SAR gets stuck on the tx side.	Shut down the interface before changing the vc-class value.
	CSCdy10649	NRP-2 L2TP Sessions/tunnel load balancing is uneven.	If the service profile has more than one gateway address, when tunnel sessions are established, these sessions are not equally distributed among all of the tunnels.	None.
	CSCdy42397	NRP-2 stops responding due to illegal address access	Periodically the NRP-2 running SSG and PPoE will stop responding or reload.	None.

Table 8   Open Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B7 (continued)

Product	Caveat ID Number	Title	Description	Workaround
NRP-2	CSCdy51419	NRP-2 performance low with Non-L2TP/PPPoX & also with MPLS-VPN	There is a performance degradation of about 10 percent with all non-L2TP protocols and MPLS VPN for small packet sizes (64, 256 & 512). The degradation seen for both ATM-ATM and GE-ATM paths.	None.
	CSCdy74242	Many FIFO resets can cause SAR to stop responding.	This can be due to a bad line or bad DSL modem.	None.
	CSCdy79231	DHCP relay option 82 contains interface 0/0/0 with VPI 0	If a user connects via the VPI 0, the nas-port from the accounting-request is set to 0 and the value of the DHCP option 82 is incorrect. For any other VPI it works correctly.	None.
	CSCdy83451	Adding dot1q/isl subif with ip vrp causes trunk flap	If you add a new subinterface configuration on the gigabit Ethernet trunk, the entire interface will flap and all existing vlans on that trunk will go down.	None.
	CSCdz05890	TXRPT_NOBUF messages and console locks-up when shut a0/0/0 sub-I/F	When you shut down the atm subinterface, TXRPT_NOBUF messages will flood the console causing it to lock-up. All sessions will then drop.	Shut down the main interface before changing the shaper's parameters.
	CSCdz24276	GigE interface stops passing traffic	Under some circumstances, the Gigabit Ethernet interface on the NRP-2 can lock up and stop transmitting data.	Flap the Gigabit Ethernet interface on the NRP-2 or clear counters.
NRP-2SV	CSCdy16900	NRP-2 SAR stuck after executing atm vc-per-vp repeatedly	This problem occurs when executing **atm vc-per-vp** commands through a script. The UUT has 3K PPPoA + 1.5K PPPoE + 500 RFC1483 sessions and 17K PPS traffic is passing in the downsteam direction. After executing the script for a couple of hours, the NRP-2-SV SAR gets stuck and the packets are received but the NRP-2-SV does not transmit them out.	Plan to use the **atm vc-per-vp** command only during administrative window. If you experience this issue, use **shut** and **no shut** on the ATM main interface.
	CSCdy73108	SAR failure at RX side	N/A	None.

Table 9 lists open caveats that pertain to MIB files for the Cisco 6400 aggregator for Release 12.2(4)B7.

Table 9   Open Caveats for Cisco 6400 Broadband Aggregator MIBs for Release 12.2(4)B7

Caveat ID Number	Description
CSCdw67048	ciscoDslProvisionMIB takes too long to timeout.

Closed and Resolved Caveats—Release 12.2(4)B7

All of the caveats listed in Table 10 are closed or resolved in Cisco IOS Release 12.2(4)B7 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)B7

Product	Caveat ID Number	Description
All	CSCdy74356	NSP stops responding while doing snmpwalk on cisco6400chassis MIB
	CSCdz06897	Superfluous radius auth request sent
NRP-1	CSCdx94482	I/O mem exhausted by normal buffers - 1600vc 50Mbps traffic.
	CSCdy11913	MPLS/VPN performance improvement
	CSCdy52638	I/O memory exhaustion by Normal Buffers
	CSCdy55752	Memory leak in I/O memory
NRP-2	CSCdx81060	8K PPPoA sess/2K L2TP tunnels not coming up w/t traffic shaping enabled
NRP-2SV	CSCdy73062	UTOPIA Rx reset check needs improvement
NSP	CSCin18520	Maplist SVC ping across a hierarchi. tunnel generates tracebacks

Open Caveats—Release 12.2(4)B6

All of the caveats listed in Table 11 are open in Cisco IOS Release 12.2(4)B6 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 11   Open Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B6

Product	Caveat ID Number	Title	Description	Workaround
All	CSCdx91120	%SYS-2_WATCHDOG: Process = PPPOE background daemon.	If a permanent virtual circuit (PVC) that is configured for PPPoX autosensing is removed, the router is sometimes reloaded due to watchdog timeout.	Determine the virtual access (VA) interface for each of the PPPoE sessions and enter **clear interface virtual-interfacexxx.** When all of the sessions on the virtual circuit are gone, the virtual circuit can be removed.
	CSCdx94482	I/O mem exhausted by normal buffers - 1600vc 50Mbps traffic.	For 1600 PPPoA VC and approximately 50 Mbps traffic, the I/O memory is exhausted. The router sends a MALLOCFAIL error and stops responding.	Reduce traffic.
	CSCdy52638	I/O memory exhaustion by Normal Buffers	When you use an RA/MPLS configuration, you may experience I/O memory exhaustion.	None.
NSP	CSCdy07600	NSP Reload when formatting slot 0	When trying to format an ATA card, the **format slot 0** command can cause the NSP to reload and failover to the redundant NSP prior to the format completing.	Do not use the **format slot** command on the NSP. Use **format disk** instead.
NRP-1	CSCdx93277	Idle timer not working correctly in 12.2(2)BX1.	On a Cisco 6400 NRP1 terminating PPPoE sessions in a PPP Termination and Aggregation (PTA) setup, the idle timer that is downloaded from the RADIUS server on the Virtual-Access interfaces associated to the PPPoE user sessions might not work correctly.	None.
	CSCdy11913	MPLS/VPN performance improvement	CRC input errors are observed under the atm0/0/0 interface of a c6400 NRP1 configured as a PE. This congestion might limit traffic performances.	None.
	CSCdy55752	Memory leak in I/O memory	For PPPoE connections to an NRP that is working in PTA mode, there can be a memory leak in I/O memory. This issue can occur even with a reduced number of users (around 70).	None.

Table 11   Open Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B6 (continued)

Product	Caveat ID Number	Title	Description	Workaround
NRP-2	CSCdu58024	NRP-2 GE<->GE back to back with no auto nego, not able to recover link.	GE interfaces of the NPR2 are connected back to back with auto negotiation turned off. Initially the connectivity works fine. However, when one of the GE ports is toggled using **no shut** and **shut**, the connectivity breaks. With auto negotiation off, the connections is not broken.	None.
	CSCdx81060	8K PPPoA sess/2K L2TP tunnels not coming up w/t traffic shaping enabled	8K PPPoA sessions over 2K L2TP tunnels are not coming up when initiated together with traffic shaping enabled.	None.
	CSCdy09155	SAR chip run out of transmit buffer link pointers.	This problem occurs only with frequent changes to the shaper value defined in vc-class. The SAR gets stuck on the tx side.	Shut down the interface before changing the vc-class value.
	CSCdy10649	NRP-2 L2TP Sessions/tunnel load balancing is uneven.	If the service profile has more than one gateway address, when tunnel sessions are established, these sessions are not equally distributed among all of the tunnels.	None.
	CSCdy42397	NRP-2 stops responding due to illegal address access	Periodically the NRP-2 running SSG and PPoE will stop responding or reload.	None.
	CSCdy51419	NRP-2 performance low with Non-L2TP/PPPoX & also with MPLS-VPN	There is a performance degradation of about 10 percent with all non-L2TP protocols and MPLS VPN for small packet sizes (64, 256 & 512). The degradation seen for both ATM-ATM and GE-ATM paths.	None.
	CSCdy74242	Many FIFO resets can cause SAR to stop responding.	This can be due to a bad line or bad DSL modem.	None.

Table 11   Open Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B6 (continued)

Product	Caveat ID Number	Title	Description	Workaround
NRP-2-SV	CSCdy16900	NRP-2 SAR stuck after executing atm vc-per-vp repeatedly	This problem occurs when executing **atm vc-per-vp** commands through a script. The UUT has 3K PPPoA + 1.5K PPPoE + 500 RFC1483 sessions and 17K PPS traffic is passing in the downsteam direction. After executing the script for a couple of hours, the NRP-2-SV SAR gets stuck and the packets are received but the NRP-2-SV does not transmit them out.	Plan to use the **atm vc-per-vp** command only during administrative window. If you experience this issue, use **shut** and **no shut** on the ATM main interface.
NRP-2SV	CSCdy73062	UTOPIA Rx reset check needs improvement	N/A	None.
	CSCdy73108	SAR failure at RX side	N/A	None.

Table 12 lists open caveats that pertain to MIB files for the Cisco 6400 Cisco 6400 aggregator for Release 12.2(4)B6.

Table 12   Open Caveats for Cisco 6400 MIBs for Release 12.2(4)B6

Caveat ID Number	Description
CSCdw67048	ciscoDslProvisionMIB takes too long to timeout.

Closed and Resolved Caveats—Release 12.2(4)B6

All of the caveats listed in Table 13 are closed or resolved in Cisco IOS Release 12.2(4)B6 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 13   Closed or Resolved Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B6

Product	Caveat ID Number	Description
All	CSCdv81807	PPTP: spurious memory access made at vpdn_bringup_vaccess
	CSCdx94396	CEF/FS, NAT failing when checking next-hop in route-map policy
	CSCdy02662	Multiple users configuring vc-class simultaneously can stop the router from responding.
	CSCdy04411	CT3_UP216 card resets due to bus error at create_dongle
	CSCdy12404	Bus Error at ip_nacl_delete
	CSCdy18641	L2TP connection to the 7401ASR (LNS), stops responding unexpectedly
	CSCdy51414	AAA: Accounting fails on 3rd login
	CSCdy56340	System stops responding when test PPPoE with traffic

Table 13 Closed or Resolved Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B6 (continued)

Product	Caveat ID Number	Description
NRP-2	CSCdx76520	port L3 parity error recovery to NRP-2.
	CSCdy51392	NRP-2 SSG goes out of mem with 8K sess (PPPoX Proxy NAT & with GRE)
NRP-2SV	CSCdy02236	PVC stops responding while changing shaper value in vc-class.

Open Caveats—Release 12.2(4)B5

All of the caveats listed in Table 14 are open in Cisco IOS Release 12.2(4)B5 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 14 Open Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B5

Product	Caveat ID Number	Title	Description	Workaround
All	CSCdx91120	%SYS-2_WATCHDOG: Process = PPPOE background daemon.	If a permanent virtual circuit (PVC) that is configured for PPPoX autosensing is removed, the router is sometimes reloaded due to watchdog timeout.	Determine the virtual access (VA) interface for each of the PPPoE sessions and enter **clear interface virtual-interfacexxx**. When all of the sessions on the virtual circuit are gone, the virtual circuit can be removed.
	CSCdx94482	I/O mem exhausted by normal buffers - 1600vc 50Mbps traffic.	For 1600 PPPoA VC and approximately 50 Mbps traffic, the I/O memory is exhausted. The router sends a MALLOCFAIL error and stops responding.	Reduce traffic.
	CSCdy52638	I/O memory exhaustion by Normal Buffers	When you use an RA/MPLS configuration, you may experience I/O memory exhaustion.	None.
NRP-1	CSCdx93277	Idle timer not working correctly in 12.2(2)BX1.	On a Cisco 6400 NRP1 terminating PPPoE sessions in a PPP Termination and Aggregation (PTA) setup, the idle timer that is downloaded from the RADIUS server on the Virtual-Access interfaces associated to the PPPoE user sessions might not work correctly.	None.
	CSCdy11913	MPLS/VPN performance improvement	CRC input errors are observed under the atm0/0/0 interface of a c6400 NRP1 configured as a PE. This congestion might limit traffic performances.	None.

Table 14   Open Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B5 (continued)

Product	Caveat ID Number	Title	Description	Workaround
NRP-2	CSCdu58024	NRP-2 GE<->GE back to back with no auto nego, not able to recover link.	GE interfaces of the NPR2 are connected back to back with auto negotiation turned off. Initially the connectivity works fine. However, when one of the GE ports is toggled using **no shut** and **shut**, the connectivity breaks. With auto negotiation off, the connections is not broken.	None.
	CSCdx76520	port L3 parity error recovery to NRP-2.	Currently all L3 cache parity errors are considered imprecise, and thus fatal.	If you are seeing frequent cache parity errors, configure cache L3 bypass and reload the router to turn off L3 caching. **Note** Frequent cache parity errors probably a sign of a board that should be removed and replaced. You might continue to run with the L3 cache turned off, but it is better to get the hardware fixed.

Table 14   Open Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B5 (continued)

Product	Caveat ID Number	Title	Description	Workaround
NRP-2	CSCdx81060	8K PPPoA sess/2K L2TP tunnels not coming up w/t traffic shaping enabled	8K PPPoA sessions over 2K L2TP tunnels are not coming up when initiated together with traffic shaping enabled.	None.
	CSCdy02662	Multiple users configuring vc-class simultaneously can cause the router to stop responding.	While modifying two VC classes involving vbr-nrt from two separate Telnet sessions, the NRP-2 stopped responding.	None.
	CSCdy09155	SAR chip run out of transmit buffer link pointers.	This problem occurs only with frequent changes to the shaper value defined in vc-class. The SAR gets stuck on the tx side.	Shut down the interface before changing the vc-class value.
	CSCdy10649	NRP-2 L2TP Sessions/tunnel load balancing is uneven.	If the service profile has more than one gateway address, when tunnel sessions are established, these sessions are not equally distributed among all of the tunnels.	None.
	CSCdy51392	NRP-2 SSG goes out of mem with 8K sess (PPPoX Proxy NAT & with GRE)	The router may run out of process memory when running 8000 PPPoA sessions over 1700 GRE tunnels. The same issue is observed with 8000 PPPoX Proxy NAT.	For PPoA over GRE, lower the supported sessions to 6000 and GRE tunnels to 1000. For PPoX Proxy NAT, lower the supported PPPoX Proxy NAT sessions to 6000.
	CSCdy51419	NRP-2 performance low with Non-L2TP/PPPoX & also with MPLS-VPN	There is a performance degradation of about 10 percent with all non-L2TP protocols and MPLS VPN for small packet sizes (64, 256 & 512). The degradation seen for both ATM-ATM and GE-ATM paths.	None.

Table 14   Open Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B5 (continued)

Product	Caveat ID Number	Title	Description	Workaround
NRP-2SV	CSCdy02236	PVC stops responding while changing shaper value in vc-class.	PVC on L2TP tunnels may get stuck if the shaper c-class value is changed.	Shut down the interface before changing the vc-class value.
	CSCdy16900	NRP-2 SAR stuck after executing atm vc-per-vp repeatedly	This problem occurs when executing **atm vc-per-vp** commands through a script. The UUT has 3K PPPoA + 1.5K PPPoE + 500 RFC1483 sessions and 17K PPS traffic is passing in the downsteam direction. After executing the script for a couple of hours, the NRP-2-SV SAR gets stuck and the packets are received but the NRP-2-SV does not transmit them out.	Plan to use the **atm vc-per-vp** command only during administrative window. If you experience this issue, use **shut** and **no shut** on the ATM main interface.
	CSCdy43534	NRP-2SV SAR stuck	NRP-2SV may sporadically stop transmitting cells.	There is no workaround. The temporary remedy is to issue **shut** and **no shut** commands on the main interface.

Table 15 lists open caveats that pertain to MIB files for the Cisco 6400 aggregator for Release 12.2(4)B5.

Table 15   Open Caveats for Cisco 6400 MIBs for Release 12.2(4)B5

Caveat ID Number	Description
CSCdw67048	ciscoDslProvisionMIB takes too long to timeout.

Closed and Resolved Caveats—Release 12.2(4)B5

All of the caveats listed in Table 16 are closed or resolved in Cisco IOS Release 12.2(4)B5 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 16   Closed or Resolved Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B5

Product	Caveat ID Number	Description
All	CSCdx65264	L2TP LAC not forwarding sessions to backup tunnels with load balancing.
	CSCdx89853	PPPoA/L2TP sess take long time to come up while changing shaper.
	CSCdx91121	Acct-Session-Id inconsistent with nas-port format d - no VC in Stop.
	CSCdy03552	Memory leak in PAM Mail box while doing wr mem from dual telnet.
	CSCdy03667	PPP Events Process takes 100% CPU with one pppoe session 12.2(04)BX.
	CSCdy05118	Restart with old-style per-user interface-config > 600 bytes.
	CSCdy07201	PPPoA sessions not coming up after modifying shaper value.
	CSCdy07797	ATM fail to modify BCS value when PPPoE session logs off.
	CSCdy09672	High logon time for adsl users.
	CSCdy12404	Bus Error at ip_nacl_delete.
	CSCdy12953	PPPoE/PPPoA autosense has 10 sec connect delay.
	CSCdy32673	NAS port prepend for the acct-sess-id(44) is missing.
	CSCdy39974	invalid L2TP control packet stops responding and breaks other vendor's devices.
	CSCdy39989	Bus Error when trying to delete ACL. Duplicate of CSCdy12404.
	CSCin10313	Tunnel Service packets sent through wrong interface.
	CSCin13289	End-to-End ping not passing for PPPoX/RBE sessions with cef enabled.
	CSCin13912	SSG:Packets to tunnel service not going through the l2tp tunnel.
NRP-1	CSCdx85599	NRP1 stops responding repeatedly with Bus Error exception in atm_get_p2pvc.
NRP-2	CSCdy03958	NRP stops responding while scaling 2k PPPoA sessions.
	CSCdy06133	NRP-2 SSG taking very long time for hosts to login.
	CSCdy18667	NRP-2SV SAR PCI R/W point mismatch
NSP	CSCdx91019	OAM end-loopback pings not working properly on NSP
	CSCdx93120	OAM pings failing with ping no match message

Open Caveats—Release 12.2(4)B3

All of the caveats listed in Table 17 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 17   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	System failure due to watchdog @ parse_radius_response.

Table 17   Open Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B3 (continued)

Product	Caveat ID Number	Description
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 NRP-2 stopped.
	CSCdr52399	NRP-2 reset during image download breaks NSP.
	CSCdr55905	config write code doesn't check for free space on disk.
	CSCdr70852	With service compress-config enabled, NRP-2 does not comp saved conf.
	CSCdr76980	NSP disk1 operation affect NRP-2 from loading image from disk0.
	CSCdt57785	NRP-2: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	NRP-2 GE<->GE back to back with no auto nego, not able to recover link.
	CSCdu66436	False Counter throughput Statistics.
	CSCdv32871	NRP-2:Cut and paste a range pvc config produces a trace back message.
	CSCdw23646	Traceback for shaping with policing.
	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 NRP-2 stops responding 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 count on NSP ATM 0/0/0 virtual interface.

Table 18 lists open caveats that pertain to MIB files for the Cisco 6400 aggregator for Release 12.2(4)B3.

Table 18   Open Caveats for Cisco 6400 MIBs for Release 12.2(4)B3

Caveat ID Number	Description
CSCdw67048	ciscoDslProvisionMIB takes too long to timeout.

Closed and Resolved Caveats—Release 12.2(4)B3

All of the caveats listed in Table 19 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 19   Closed or Resolved Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B3

Product	Caveat ID Number	Description
All	CSCdx24528	PPP Packet redirected to same interface in endless loop.
NRP-1, NRP-2, NRP-2SV	CSCdv29433	Router stops responding when set any command is 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.
NRP-1	CSCdm92848	EHSA minor alarm pop up after 2 non-redundancy NRP boot up.
	CSCdp05523	NAT:Large address range and 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 fails with BADFREEMAGIC message.
	CSCdu09764	c6400:NRP fails with bad magic on allocated block.
	CSCdu56256	Fast ethernet interface reports %AMDP2_FE-3-UNDERFLO, trnsmit error.
	CSCdu64354	Option 82 and Radius VPI/VCI authentication do not work with S-PVC.
	CSCdv63811	Memory corruption in I/O pool.
	CSCdv74851	NRP1 with IRB fails with bus error.
	CSCdv82697	NRP1:IRB Routing protocol updates not working with ISIS.
	CSCdw59637	With oam enabled, atm subinterface up/down after reload.
	CSCdw66951	Tunnel user 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 currently only on 7200 & rsp).

Table 19   Closed or Resolved Caveats for Cisco 6400 NRP and NSP for Release 12.2(4)B3 (continued)

Product	Caveat ID Number	Description
NRP-2, NRP-2SV	CSCdr70852	With service compress-config enabled, NRP-2 does not comp saved conf.
	CSCdr76980	NSP disk1 operation affect NRP-2 from loading image from disk0.
	CSCdr83804	ROMMON: NRP-2 fails if NSPs disk0 is removed during NRP-2 idnld.
	CSCdr95295	NRP-2: total memory size displayed is incorrect.
	CSCdu69223	Buffer leak in PAM MBOX.
	CSCdv55811	NRP-2 fails @se64_close_rx_vc_desc when trying to change vc encap
	CSCdv75114	NRP-2: ISIS routing updates not sent with AAL5NLPID, SNAP, MUX in GE-ATM.
	CSCdw13019	Loss of IP/SNMP connectivity to NRP-2 when NSP has large run-conf.
	CSCdw30583	Loss of IP connectivity between NSP and NRP-2 with big config files.
	CSCdw32965	NRP-2 stops responding when traffic switched over from another NRP-2.
	CSCdw37740	Heavy loading causes NSP can't ping atm OAM to NRP-2.
	CSCdw60122	OAM CRC10 error 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 NRP-2(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 stops responding while scaling PPPoA sessions over GRE tunnels.
	CSCdw49074	NRP-2 fails while scaling 8k PPPoA Sessions over 2k GRE tunnels.
	CSCdw54156	NRP SSG L2TP/PPPoX tunnel sessions drops with traffic.
	CSCdw79480	Not able to scale 4000 SSG hosts logged into 2000 L2TP tunnel services.
	CSCdx06795	NRP-2 SSG PPPoX/L2TP tunnel sessions drop with traffic GE-ATM path.

Table 20 lists resolved caveats that pertain to MIB files for the Cisco 6400 aggregator for Release 12.2(4)B3.

Table 20   Closed or Resolved Caveats for Cisco 6400 MIBs for Release 12.2(4)B3

Caveat ID Number	Description
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 NRP-2 when NSP has large run-conf.
CSCdw52894	NRP stops responding while walking the cdslVcClassTable.
CSCdw71419	ciscoFlashFileTable loops while doing an SNMP walk.
CSCdw80181	Watchdog timer expired.

Table 20   Closed or Resolved Caveats for Cisco 6400 MIBs for Release 12.2(4)B3

Caveat ID Number	Description
CSCdw85034	Memory leak in CISCO-DSL-PROVISION-MIB.
CSCdw86632	Getnext returns uninstantiated objects in the CISCO-ATM2-MIB.

Open Caveats—Release 12.2(2)B7

All of the caveats listed in Table 21 are open in Cisco IOS Release 12.2(2)B7 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 21   Open Caveats for Cisco 6400 NRP and NSP for Release 12.2(2)B7

Product	Caveat ID Number	Description
NRP-2, NRP-2SV, NRP-1, and NSP	CSCdx53637	High CPU utilization for PPPoA sessions recovery when modify shaper
NRP-2	CSCdz32636	sub i/f flap causes traceback messages

Closed and Resolved Caveats—Release 12.2(2)B7

All of the caveats listed in Table 22 are closed or resolved in Cisco IOS Release 12.2(2)B7 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 22   Closed or Resolved Caveats for Cisco 6400 NRP and NSP for Release 12.2(2)B7

Product	Caveat ID Number	Description
All	CSCdu41289	Error: Bad DFS cluster data passed occurs when deleted from data disk
	CSCdw18198	Parser cache entry may get deleted when in use
	CSCdw47129	Utopia Interface may be in disabled state
	CSCdy27667	Use OAM-Ping to detect/recover the SAR hangup issues
	CSCdy35644	SAR workaround for dx51200 need improve
	CSCdy61412	PPPoE crashes NRP-2 configured with Autosense
	CSCdy74356	NSP crashes while doing snmpwalk on cisco6400chassis MIB
	CSCdy88743	no protocol ip inarp disappears from config after reload
NRP-2, NRP-2SV, NRP-1, and NSP	CSCdx38290	Multiple users configuring vc-class simultaneously causes router to stop responding.

Table 22   Closed or Resolved Caveats for Cisco 6400 NRP and NSP for Release 12.2(2)B7 (continued)

Product	Caveat ID Number	Description
NRP-2, NRP-2SV	CSCdx49484	NRP-2: underflow message while passing traffic through shaped ppp session
	CSCdx56935	Configuring 8 shapers on NRP-2SV makes VCs UNACTIVE,out of rate queue
	CSCdx61271	The atm vc count shows as 0 with 8K sessions & 7 shaper configured
	CSCdx62483	NRP-2:SAR stuck while changing shaping value.
	CSCdx62435	NRP-2: negative VC count, when shut atm int after changing shaper val
	CSCdx81060	8K PPPoA sess/2K L2TP tunnel not coming up w/t traffic shaping enabled
	CSCdx89853	PPPoA/L2TP session takes a long time to appear while changing shaper
	CSCdx92449	With CEF ON, Input atm0/0/0 traffic is not displayed correctly
NRP1	CSCdw12730	NRP stops responding with corrupted PC on parse_token with DT special
NRP-2	CSCdy39288	NRP-2: spurious-memory-access traceback while passing traffic
	CSCdy73108	NRP-2SP (SAR rev D): SAR failure at RX side
	CSCdy74242	Many FIFO resets can cause SAR to hang.
	CSCin21529	NRP-2 crashing and reloading infinitely after wr erase+reload
NRP-2SV	CSCdy18667	NRP-2SV SAR PCI R/W point mismatch
	CSCdy73062	NRP-2: UTOPIA Rx reset check needs improvement
	CSCdz05890	TXRPT_NOBUF messages and console locks-up when shut a0/0/0 sub-I/F
	CSCdz19789	Add CLIs and Reset Default Values for the SAR E with Metal Fixes
	CSCin20239	Shaping accuracy is low
NSP	CSCdv39868	Assertion failed error on console during debugs
	CSCdx91019	OAM end-loopback pings not working properly on NSP
	CSCdx93120	OAM pings failing with ping no match message

Open Caveats—Release 12.2(2)B6

All of the caveats listed in Table 23 are open in Cisco IOS Release 12.2(2)B6 for the Cisco 6400 NRP-2, Cisco 6400 NRP-2SV, Cisco 6400 NRP-1, and the Cisco 6400 NSP.

Table 23   Open Caveats for Cisco 6400 NRP and Cisco 6400 NSP for Release 12.2(2)B6

Product	Caveat ID Number	Description
NRP-2, NRP-2SV	CSCdx49484	NRP-2: underflow message while passing traff through shaped PPP session.
	CSCdx56935	Configuring 8 shapers on NRP-2SV makes VCs UNACTIVE,out of rate queue
	CSCdx61271	The atm vc count shows as 0 with 8K sessions and 7 shaper configured
	CSCdx62435	NRP-2: negative VC count, when shut atm int after changing shaper val
	CSCdx62483	NRP-2:SAR stuck while changing shaping value.
	CSCdx81060	8K PPPoA sess/2K L2TP tunnel not coming up without traffic shaping enabled
	CSCdx89853	PPPoA/L2TP session takes a long time to appear while changing shaper
	CSCdx92449	With CEF ON, Input atm0/0/0 traffic is not displayed correctly

Table 23   Open Caveats for Cisco 6400 NRP and Cisco 6400 NSP for Release 12.2(2)B6

Product	Caveat ID Number	Description
NRP-2, NRP-2SV, NRP-1, and NSP	CSCdx38290	Multiple users configuring VC class simultaneously can cause the router to stop responding
	CSCdx53637	High CPU utilization for PPPoA sessions recovery when shaper is modified
SSG	CSCdx94295	Dynamic MTU check for L2TP feature is not working with Boron

Closed or Resolved Caveats—Release 12.2(2)B6

All of the caveats listed in Table 24 are closed or resolved in Cisco IOS Release 12.2(2)B6 for the Cisco 6400 NRP-2, Cisco 6400 NRP-2SV, Cisco 6400 NRP-1, and the Cisco 6400 NSP.

Table 24   Closed or Resolved Caveats for Cisco 6400 NRP and Cisco 6400 NSP for Release 12.2(2)B6

Product	Caveat ID Number	Description
NRP-2, NRP-2SV	CSCdx29110	NRP-2 input queue wedge when receiving OAM traffic
	CSCdx31956	CPU stops responding when performing interface shut/no shut frequently
	CSCdx45918	NRP-2SV with traffic shaping: SAR short fetch issue. SAR stops responding.
	CSCdx49465	CPUHOG at process=pool manager with traffic
	CSCdx51200	NRP-2 PVC stops responding when traffic travels through this shaped VC
	CSCdx54883	I/O memory completely depleted when traffic is sent overnight
	CSCdx62210	NRP-2 stops responding during stressful configuring ATM VCs
	CSCdx62263	Performance degradation with Traffic GE (ATM with shaping on)
	CSCdx68380	NRP-2 ATM transmit queue stops responding
	CSCdx70100	Port CSCdu24077 to NRP2 to suppress cache parity errors
NRP-1	CSCdw73249	SAR not setting up VC when VC line protocol is down
NRP-2, NRP-2SV, NRP-1, and NSP	CSCdt60558	Cisco 10000 series Edge Services Router (ESR) scalability: atm_vpivci_to_vc function is not scalable
	CSCdv48261	Improvements to dynamic ACLs for Cisco IOS fw
	CSCdv79009	Access-class on VTY denies all telnet sessions coming into VRF int.
	CSCdw11331	NSP crash with TLB exception and Traceback message
	CSCdw19522	Router restarts due to bus error @ dhcpd_destroy_binding
	CSCdw25402	RPM-PR card crashed when provisioning bulk connections from CWM
	CSCdx63798	NAS port prepend for the acct-sess-id(44) is missing
MIBs	CSCdv02925	Memory leak in CISCO-ATM-SWITCH-CUG-MIB
	CSCdv83902	SNMP timeouts walking ciscoPppoeMIB
	CSCdw13019	Loss of IP/SNMP connectivity to NRP2 when NSP has large run-conf

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 12.2T*, which is located on Cisco.com and the Documentation CD-ROM.

Closed or Resolved Caveats—Release 12.2(2)B5

All of the caveats listed in Table 25 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 25   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 fails while walking the cdslVcClassTable.
	CSCdw68465	NRP-1: memory corruption in vpdn session failure recording.
NRP-2, NRP-2SV, NRP-1, and NSP	CSCdv66216	EE48: ST:RP stopped responding while it attempted to remove 48 VPNs from 48 DS3 interface.
	CSCdv83883	Spurious memory while 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.

Closed or Resolved Caveats—Release 12.2(2)B4

All of the caveats listed in Table 26 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 26   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	Enhance ATM driver debugging.
NRP-1 and NSP	CSCdv74851	NRP1 with IRB fails with bus error.
	CSCdw05710	Cisco 6400 aggregator: PVC becomes inactive, %ATMCES-1-ERRCREATEVC.
	CSCdw81924	Port CSCdm89718 to NRP1 (code currently only on Cisco 7200 series router and rsp).

Table 26   Closed or Resolved Caveats for Cisco 6400 NRP and Cisco 6400 NSP for Release 12.2(2)B4 (continued)

Product	Caveat ID Number	Description
NRP-2, NRP-2SV, NRP-1, and NSP	CSCdw42849	PPPoE session does not clear.
	CSCdw65903	An error can occur with management protocol processing.

Open Caveats—Release 12.2(2)B3

All of the caveats listed in Table 27 are open in Cisco IOS Release 12.2(2)B3 for the Cisco 6400 NRP-2 and NRP-2SV.

Table 27   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 NRP-2 when NSP has large run-conf.
	CSCdw26218	Virtual access gets stuck in LCP closed state.
	CSCdw30583	Loss of IP connectivity between NSP and NRP-2 with large config files.
	CSCdw32965	NRP-2 stops responding when traffic switches over from another NRP-2.
	CSCdw37740	Heavy loading prevents NSP from pinging ATM OAM to NRP-2.

Closed or Resolved Caveats—Release 12.2(2)B3

All of the caveats listed in Table 28 are closed or resolved in Cisco IOS Release 12.2(2)B3 for the Cisco 6400 NRP-2 and NRP-2SV.

Table 28   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: Contains a possible dereference null pointer.
	CSCdw11239	PE of MPLS-VPN stops forwarding packets after stress with large packet sizes.
	CSCdw37282	Traffic does not pass when reset occurs with traffic shaping enabled.

Open Caveats—Release 12.2(2)B2

All of the caveats listed in Table 29 are open in Cisco IOS Release 12.2(2)B2 for the Cisco 6400 NRP-1, NRP-2, and NRP-2SV. All of the caveats listed in Table 30 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 31 lists caveats that pertain to MIB files for the Cisco 6400 for Release 12.2(2)B2.

Table 29 Open Caveats for Cisco 6400 NRP for Release 12.2(2)B2

Product	Caveat ID Number	Description
NRP-2	CSCdr95295	NRP-2: Total memory size displayed is incorrect.
	CSCdt57785	NRP-2: You cannot view startup config context if config is set to 0x**4*.
	CSCdu58024	NRP-2: GE<->GE back to back with no autonegotiation and user is unable to recover link.
	CSCdu58091	A copy of files from NRP-2 to NSP causes an NSP Bus Error exception.
	CSCdu66436	False counter throughput statistics.
	CSCdv32871	NRP-2: Cut and paste a range pvc config produces a traceback message.
	CSCdv39868	Assertion failed error on console during debugs.
	CSCdv55745	If you try to change encap type, the error message Null RX particle header appears.
	CSCdv55811	NRP-2 stops responding at se64_close_rx_vc_desc if you try to change vc encap.
	CSCdv56280	GE: Auto-nego CLI command is missing.
	CSCdv70703	NRP-2: After removing the multicast boundary mroute table not updated.
	CSCdv75114	NRP-2: ISIS routing updates not sent with AAL5NLPID, SNAP, MUX in GE-ATM.
	CSCdv77023	NRP-2: Multicast client does not respond to ICMP packet with CEF ON.
	CSCdw07107	When NSP has large run-conf, there is a loss of IP/SNMP connectivity to NRP-2.
NRP-1	CSCdp05523	NAT: Large address range and portlist chains cause CPU spikes.
	CSCdp59354	Egress traffic to RBE ints process sw with FE+ISL and <<bridge irb>>.
	CSCdr04534	PPPoA/L2TP: 2000 sessions. Some connected routes are not established after flap.
	CSCdr50376	Some sessions drop when the VCs are oversubscribed.
	CSCdr82324	L2TP: VPDN: Releases idb for LAC/LNS tunnel.
	CSCdt74755	NAT cause high CPU utilization.
	CSCdu01557	NRP fails with BADFREEMAGIC message.
	CSCdu09764	c6400: NRP crash with bad magic on allocated block.
	CSCdu56256	Fast Ethernet interface reports %AMDP2_FE-3-UNDERFLO, transmit error.
	CSCdu64354	Option 82 and RADIUS VPI/VCI authentication does not work with S-PVC.
	CSCdv19996	FE interface on some NRP-1 boards drops packets.
	CSCdv63811	Memory corruption in I/O pool.
	CSCdv74851	NRP-1 with IRB fails with bus error.
	CSCdv75177	NRP-1-PPPoA—Poor traffic performances caused by ATM0/0/0 drops.
	CSCdv82697	NRP-1: IRB Routing protocol updates not working with ISIS.
SSG	CSCdv05136	SSG Service Profile Name should be legally formatted.

Table 30   Open Caveats for Cisco 6400 NSP for Release 12.2(2)B2

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

Table 31   Open Caveats for Cisco 6400 MIBs for Release 12.2(2)B2

Caveat ID Number	Description
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 of the caveats listed in Table 32 are closed or resolved in Cisco IOS Release 12.2(2)B2 for the Cisco 6400 NRP-1 and NRP-2. All of the caveats listed in Table 33 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 32   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 32   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 appears after two non-redundancy NRP bootups.
	CSCdr88742	wr mem on NRP2 does not generate a warning or error message if no disk0.
	CSCdr98773	Creating subinterfaces and PVCs does not appear in the configuration file.
	CSCds26319	VA interfaces counters show three times the actual counts if the client is NRP2.
	CSCds47327	NRP2_SE64-3-ULD_BADVC message if you issue the **shut atm sub-interface** commands.
	CSCds79849	CPUHOG while clearing counters with large numbers of PPP sessions.
	CSCds83542	Spurious Memory access during PPPOA/L2TP sessions.
	CSCds83689	NRP2: Some sessions 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 clear counters are being processed.
	CSCdt37234	ATM0/0/0 stops passing traffic on the NRP2 in Cisco IOS Release 12.1(4.4)DC1.
	CSCdt51547	Packet drop with ip verify unicast reverse-path.
	CSCdt51810	Crash at nrp_ip2_tag_feature in Cisco IOS Release 12.1(5)DC throttle.
	CSCdt65960	Access-list not working on VTY when you telnet GigEth port.
NRP-1	CSCdv47420	NRP1 Ethernet interface does not receive a dynamic IP address.
	CSCdv51304	Option 82 is not removed from unnumbered DHCP responses.
	CSCdv57549	NRP1 FE interface enters reset state.
SSG	CSCdt73695	SSG HTTP Redirection feature does not work for RBE user.
	CSCdt76953	Memory leaks occur in Net Background processes when you log on to ssg l2tp.

Table 33   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 does not generate a warning or error message when no disk0.
	CSCds51415	PAM mailbox configuration not valid on NRP1 while booting.
	CSCdt29127	ILMI failure on atm0/0/0 after NSP switchover.
	CSCdt45629	Problem with VC resource allocation.
	CSCdt46373	Rwait is not cleaned up. Problem with VC management.
	CSCdt47730	OSPF and XtagATM interface issues on NRP when NSP reloads.
	CSCdt65698	NSP switchover causes NRP2 in certain slots to reset.
	CSCdt71049	APS unidirectional switches bidirectionally.
	CSCdt71080	APS forced switch to non-operational protect should not be allowed.
	CSCdt76617	PVCs on NSP subinterface stops passing traffic after reload.

Related Documentation

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

- Release-Specific Documents, page 56
- Platform-Specific Documents, page 56
- Cisco IOS Release 12.2 Documentation Set, page 57

Release-Specific Documents

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

- *Cross-Platform Release Notes*

  On Cisco.com at:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_release_notes_list.html

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

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_alerts_news.html

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

  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 12.2T*, which contain caveats applicable to all platforms for all maintenance releases of Release 12.2.

  On Cisco.com:

  Caveats for Cisco IOS Release 12.2T
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/prod_release_note09186a00800a84d7.html

  Caveats for Cisco IOS Release 12.2
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_release_note09186a00800ab6bb.html

Platform-Specific Documents

The documents listed in this section are available for the Cisco 6400 aggregator on Cisco.com and the Documentation CD-ROM. To access Cisco 6400 aggregator documentation on Cisco.com, go to http://www.cisco.com/en/US/products/hw/routers/ps314/index.html

- *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 34 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in both electronic and printed form. This documentation is available on Cisco.com at http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/index.html

Table 34   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 34   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 34   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 12.2T-Based Limited Lifetime Releases* • *New Features in Release 12.2T* • *Release Notes* (release note and caveat documentation for 12.2T-based releases and various platforms)	

Obtaining Documentation

These 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 this URL:

http://www.cisco.com

Translated documentation is available at this 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

You can order Cisco documentation in these ways:

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

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

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

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

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

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

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

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online 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 with these tasks:

- 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

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

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

Cisco TAC inquiries 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.

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

Cisco TAC Web Site

You can use the Cisco TAC Web Site 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 this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service 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 this URL to register:

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

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

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. 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 automatically opens a case.

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

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

Before calling, 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). When you call the center, have your service agreement number and your product serial number available.