



TPRelease Notes for Cisco 6400 NRP for Cisco IOS Release 12.1(5) DC

February 18, 2002

Cisco IOS Release 12.1(5) DC2

78-10959-04 Rev. B0

These release notes for the Cisco 6400 node route processor (NRP) describe the enhancements provided in Cisco IOS Release 12.1(5) DC2. These release notes are updated as needed.

For a list of the software caveats that apply to Release 12.1(5) DC2, see the [“Software Caveats” section on page 28](#) and *Caveats for Cisco IOS Release 12.1 T*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Use these release notes in conjunction with the cross-platform *Release Notes for Cisco IOS Release 12.1* located on Cisco.com and the Documentation CD-ROM.



Note

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

Contents

These release notes describe the following topics:

- [System Requirements, page 2](#)
- [New and Changed Information, page 8](#)
- [Limitations and Restrictions, page 22](#)
- [Important Notes, page 23](#)
- [Software Caveats, page 28](#)
- [Preexisting NRP-1 Hardware Caveats, page 44](#)
- [Related Documentation, page 47](#)



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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

78-10959-04 Rev. B0

- [Obtaining Documentation, page 54](#)
- [Obtaining Technical Assistance, page 55](#)

System Requirements

This section describes the system requirements for Cisco IOS Release 12.1(5) DC2 and includes the following sections:

- [Memory Recommendations, page 2](#)
- [Supported Hardware, page 3](#)
- [Software Compatibility, page 3](#)
- [Determining the Software Version, page 3](#)
- [Upgrading to a New Software Release, page 3](#)
- [Feature Tables, page 4](#)

Memory Recommendations

[Table 1](#) lists the memory recommendations for the NRP-1 and NRP-2.

Table 1 *Memory Recommendations for the Cisco 6400 NRP-1 and NRP-2*

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



Note

In most NRP-1 configurations, 64 MB DRAM is adequate for up to 750 sessions. More sessions require 128 MB DRAM. Using the NRP-1, for an upgrade from an earlier release to Cisco IOS Release 12.1(5) DC2, 128 MB DRAM is recommended.



Note

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

Supported Hardware

Cisco IOS Release 12.1(5) DC2 supports the Cisco 6400 NRP-1 and NRP-2. For detailed descriptions of the new hardware features, see the “[New and Changed Information](#)” section on page 8 and the “[Related Documentation](#)” section on page 47.

Software Compatibility

Cisco recommends that Cisco IOS Release 12.1(5) DC2 be used concurrently with Cisco IOS Release 12.1(5)DB for the Cisco 6400 node switch processor (NSP). For information about Release 12.1(5)DB for the NSP, see the *Release Notes for Cisco 6400 Node Switch Processor (NSP) for Cisco IOS Release 12.1(5)DB*.

For NRP-Service Selection Gateway (SSG) users, Cisco IOS Release 12.1(5) DC2 works with the Cisco Service Selection Dashboard (SSD) version 2.5(1) that supports the Single-Host Logon feature.

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 12.1(5) DC2, EARLY DEPLOYMENT
RELEASE SOFTWARE (fc1)
```

The output 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 Universal Access Concentrator (UAC), including upgrading a single- or dual-NRP system to a new software release, see the software note *Upgrading Software on the 6400 UAC* located at http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/softnote/upgradsw.htm

For general information about upgrading to a new software release, see the Software Advisor located at: <http://tools.cisco.com/Support/Fusion/FusionHome.do>

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

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

This product bulletin does not contain information specific to Cisco IOS Release 12.1 DC but provides generic upgrade information that may apply to Cisco IOS Release 12.1 DC.

Feature Tables

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

Table 2 lists the features supported by the Cisco 6400 NRP images in this release.



Note

This table might not be cumulative or list all the features in each image. You can find the most current Cisco IOS documentation on Cisco.com. This set of electronic documents might contain updates and modifications made after the hard-copy documents were printed.

Table 2 Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.1(5) DC2

Feature	NRP-1	NRP-2
	Supported as of Cisco IOS Release	Supported as of Cisco IOS Release
Access Protocols		
Integrated Routing and Bridging (IRB)	12.0(3)DC	12.1(4)DC
Multilink Point-to-Point Protocol (MLPPP or MLP)	12.1(3)DC	12.1(4)DC
PPP ¹ IPCP ² Subnet Negotiation	12.0(5)DC	12.1(4)DC
PPP over ATM (PPPoA) terminated	12.0(3)DC	12.1(4)DC
PPP over Ethernet (PPPoE) terminated	12.0(3)DC	12.1(4)DC
PPPoA/oE autosense (SNAP ³)	12.1(1)DC	12.1(5)DC
Routed bridge encapsulation (RBE)	12.0(5)DC	12.1(4)DC
RBE Subinterface Grouping	12.1(4)DC	12.1(4)DC
RBE unnumbered DHCP ⁴	12.1(1)DC	12.1(4)DC
RBE with DHCP	12.0(5)DC	12.1(4)DC
RBE with DHCP Option 82	12.1(5)DC	12.1(5)DC
RFC 1483 bridging	12.0(3)DC	12.1(4)DC
RFC 1483 routing	12.0(3)DC	12.1(4)DC
VC ⁵ Traffic Shaping	12.0(3)DC	Not yet supported
Aggregation and Virtual Private Networks (VPN)		
IP ⁶ Overlapping address pools (AOP)	12.1(5)DC	Not yet supported
L2TP ⁷ Multi-Hop	12.1(1)DC	12.1(4)DC

Table 2 Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.1(5) DC2

Feature	NRP-1	NRP-2
	Supported as of Cisco IOS Release	Supported as of Cisco IOS Release
L2TP tunnel service authorization enhancement	12.1(1)DC	12.1(4)DC
L2TP tunnel sharing	12.1(1)DC	12.1(4)DC
L2TP tunnel switching ⁸	12.1(1)DC	12.1(4)DC
MPLS ⁹ Edge Label Switch Router (Edge LSR)	12.0(7)DC	Not yet supported
MPLS Label Switch Controller (LSC) for BPX	12.0(7)DC	Not yet supported
MPLS VPNs ¹⁰	12.0(7)DC	Not yet supported
PPPoA tunneled into L2TP	12.0(5)DC	12.1(4)DC
PPPoE tunneled into L2TP	12.0(5)DC	12.1(4)DC
Remote Access into MPLS VPN	12.1(5)DC	Not yet supported
RFC 1577	12.0(3)DC	12.1(4)DC
VLAN ¹¹ (ISL ¹²) on NRP	12.0(3)DC	12.1(4)DC
VLAN (802.1q) on NRP-2 GE ¹³	Not applicable	12.1(5)DC
Configuration and Monitoring		
ATM ¹⁴ PVC ¹⁵ Range Command	12.1(4)DC	12.1(4)DC
Per VC error display	12.1(3)DC	12.1(5)DC
Hardware Support		
ATM (OC-3, OC-12, DS3) Interfaces	12.0(3)DC	12.1(4)DC
FE ¹⁶ Interface: 10/100 auto-negotiation, auto-sensing	12.0(3)DC	Not applicable
GE Interface	Not applicable	12.1(5)DC
Network Management Ethernet (NME)	12.0(5)DC	12.1(4)DC
NRP 1+1 Redundancy	12.0(3)DC	Not yet supported
IP and Routing		
Address Resolution Protocol (ARP)	12.0(3)DC	12.1(4)DC
Border Gateway Protocol version 4 (BGP4)	12.0(3)DC	12.1(4)DC
Enhanced Interior Gateway Routing Protocol (EIGRP)	12.0(3)DC	12.1(4)DC
Generic routing encapsulation (GRE)	12.0(3)DC	12.1(4)DC
Internet Group Management Protocol (IGMP)	12.0(3)DC	12.1(4)DC
Internet Protocol (IP) forwarding	12.0(3)DC	12.1(4)DC
IP multicast	12.0(3)DC	12.1(4)DC
Intermediate System-to-Intermediate System (IS-IS)	12.0(3)DC	12.1(4)DC
Network Address Translation (NAT) support for NetMeeting Directory	12.0(3)DC	12.1(4)DC
NetFlow for RFC1483 into MPLS VPN	12.1(5)DC	Not yet supported
Open Shortest Path First (OSPF)	12.0(3)DC	12.1(4)DC
PIM ¹⁷ Dense Mode & Sparse Mode	12.0(3)DC	12.1(4)DC

Table 2 Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.1(5) DC2

Feature	NRP-1	NRP-2
	Supported as of Cisco IOS Release	Supported as of Cisco IOS Release
Routing Information Protocol (RIP)/RIP v2	12.0(3)DC	12.1(4)DC
Transmission Control Protocol (TCP)	12.0(3)DC	12.1(4)DC
Telnet	12.0(3)DC	12.1(4)DC
Trivial File Transfer Protocol (TFTP)	12.0(3)DC	12.1(4)DC
Transparent Bridging	12.0(3)DC	12.1(4)DC
User Datagram Protocol (UDP)	12.0(3)DC	12.1(4)DC
Web Cache Coordination Protocol (WCCP) version 1	12.0(3)DC	12.1(4)DC
WCCP (v2)	12.0(7)DC	12.1(4)DC
Network Management		
Simple Network Management Protocol (SNMP) (v1, v2, and v3)	12.0(3)DC	12.1(4)DC
RADIUS/AAA		
Password Authentication Protocol (PAP)/Challenge Handshake Authentication Protocol (CHAP)	12.0(3)DC	12.1(4)DC
Remote Authentication Dial-In User Service (RADIUS)	12.0(3)DC	12.1(4)DC
RADIUS Attribute 8 (Framed-IP-Address) in Access Requests (IP Hint)	12.1(3)DC	12.1(4)DC
Terminal Access Controller Access Control System Plus (TACACS+) (admin login only)	12.0(3)DC	12.1(4)DC
VPI ¹⁸ /VCI ¹⁹ RADIUS Request and RADIUS Accounting for PPPoA	12.0(3)DC	12.1(5)DC
VPI/VCI in RADIUS Request and RADIUS Accounting for PPPoE	12.1(1)DC	12.1(5)DC
Scalability and performance		
GRE Cisco express forwarding (CEF)	12.1(1)DC	12.1(5)DC
LAC ²⁰ CEF switching	12.1(3)DC	12.1(4)DC
L2TP sessions per tunnel limiting	12.1(1)DC	12.1(4)DC
NAT CEF switching	12.1(1)DC	12.1(4)DC
Per VC buffer management	12.1(1)DC	12.1(4)DC
PPPoA CEF	12.1(1)DC	12.1(4)DC
PPPoE Fast Switching for Multicast	12.1(1)DC	12.1(5)DC
RBE CEF switching	12.1(5)DC	12.1(5)DC
Service Selection Gateway (NRP-SSG)		
PPP Aggregation Termination over Multiple Domains (PTA-MD)	12.0(3)DC	12.1(4)DC
RADIUS Interim Accounting	12.0(5)DC	12.1(4)DC

Table 2 *Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.1(5) DC2*

Feature	NRP-1	NRP-2
	Supported as of Cisco IOS Release	Supported as of Cisco IOS Release
SSG Automatic Service Logon	12.0(3)DC	12.1(4)DC
SSG CEF Switching	12.0(5)DC	12.1(4)DC
SSG Default Network	12.0(3)DC	12.1(4)DC
SSG DNS ²¹ Fault Tolerance	12.0(3)DC	12.1(4)DC
SSG enable (default is disabled)	12.0(7)DC	12.1(4)DC
SSG full username RADIUS attribute	12.1(3)DC	12.1(4)DC
SSG HTTP ²² Redirect (Phase 1)	12.1(5)DC	12.1(5)DC
SSG Cisco IOS NAT support	12.0(5)DC	12.1(4)DC
SSG Local Forwarding	12.1(1)DC	12.1(5)DC
SSG Open Garden	12.1(5)DC	12.1(5)DC
SSG Passthrough and Proxy Service	12.0(3)DC	12.1(4)DC
SSG Sequential and Concurrent Service	12.0(3)DC	12.1(4)DC
SSG Service Defined Cookie	12.1(3)DC	12.1(4)DC
SSG single host logon	12.1(3)DC	12.1(4)DC
SSG with GRE	12.0(3)DC	12.1(5)DC
SSG with Multicast	12.0(3)DC	12.1(4)DC
SSG with L2TP Service Type	12.0(7)DC	12.1(4)DC
VPI/VCI Static binding to a Service Profile	12.0(5)DC	12.1(4)DC
WebSelection	12.0(3)DC	12.1(4)DC

Table 2 Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.1(5) DC2

Feature	NRP-1	NRP-2
	Supported as of Cisco IOS Release	Supported as of Cisco IOS Release
Other Features and Feature Enhancements		
Segmentation and Reassembly Buffer Management Enhancements	12.1(1)DC	Not applicable
Session Scalability Enhancements	12.1(1)DC	12.1(4)DC

1. PPP = Point-to-Point Protocol
2. IPCP = Internet Protocol Control Protocol
3. SNAP = Subnetwork Access Protocol
4. DHCP = Dynamic Host Configuration Protocol
5. VC = virtual circuit
6. IP = Internet Protocol
7. L2TP = Layer 2 Tunneling Protocol
8. In Cisco IOS Release 12.1(5)DC, L2TP tunnel switching for the NRP-2 has been tested and is supported at the same session and tunnel levels as the NRP-1. For more information, see [Table 5 on page 23](#).
9. MPLS = Multiprotocol Label Switching
10. VPN = Virtual Private Network
11. VLAN = Virtual LAN
12. ISL = Inter-Switch Link
13. GE = Gigabit Ethernet
14. ATM = Asynchronous Transfer Mode
15. PVC = permanent virtual circuit
16. FE = Fast Ethernet
17. PIM = Protocol Independent Multicast
18. VPI = Virtual path identifier
19. VCI = Virtual channel identifier
20. LAC = L2TP access concentrator
21. DNS = Domain Name System
22. HTTP = Hypertext Transfer Protocol

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 6400 NRP for Release 12.1(5) DC2.



Note

Most of the features documented in this section have a feature module. For information about feature modules, see the [“Feature Modules” section on page 50](#).

New Hardware and Software Features Supported in Release 12.1(5)DC2

No new hardware and software features are supported by the Cisco 6400 NRP for Cisco IOS Release 12.1(5)DC2.

New Hardware and Software Features Supported in Release 12.1(5)DC1

No new hardware and software features are supported by the Cisco 6400 NRP for Cisco IOS Release 12.1(5)DC1.

New Hardware Features Supported in Release 12.1(5)DC

The following new hardware features are supported by the Cisco 6400 NRP for Cisco IOS Release 12.1(5)DC.

Gigabit Ethernet Interface (NRP-2 only)

As of Cisco IOS Release 12.1(5)DC, the Gigabit Ethernet (GE) interface on the NRP-2 is supported. The GE interface complies with the IEEE 802.3z specification and requires the appropriate Gigabit Interface Converter (GBIC) and optical fiber cable to enable one of the following connections:

- 1000BASE-SX (short wavelength)—Full-duplex operation with short-wavelength (850-nm) devices over multimode optical-fiber link spans of up to 1804 feet (550 m).
- 1000BASE-LX/LH (long wavelength/long haul)—Full-duplex operation with long-wavelength (1300-nm) devices over multimode or single-mode optical fiber. This enhancement to the IEEE 802.3z standard complies with the IEEE 802.3z 1000BASE-LX specification but extends the transmission distance up to 6.2 miles (10 km).
- 1000BASE-ZX (extended wavelength)—Full-duplex operation with extended-wavelength (1550-nm) devices over single-mode optical-fiber link spans of up to 43.5 miles (70 km). Link spans of up to 100 km are possible using premium single-mode fiber or dispersion-shifted single-mode fiber.

The GE interface supports auto-negotiation, flow-control, On-line Insertion and Removal (OIR), MAC and Drive loopback control, 802.1Q encapsulation over GE, and ISL encapsulation over GE.

The GE interface uses the same CLI commands as the Gigabit Ethernet Port Adapter for the Cisco 7200 series routers. For information about these commands, see the *Gigabit Ethernet Port Adapter* feature module at

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121e/121e4/gepa.htm>.

For information on the GBICs, see the *Gigabit Interface Converter Installation Instructions for the Cisco 6400 NRP-2 Module* at

http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/hardnote/nrp2gbic.htm.

New Software Features Supported in Release 12.1(5)DC

The following new software features are supported by the Cisco 6400 NRP for Cisco IOS Release 12.1(5)DC.

8000 PPPoE Sessions Terminated on NRP-2

As of Cisco IOS Release 12.1(5)DC, 8000 PPPoE sessions are supported on a single NRP-2 for the following configuration:

- PPPoE sessions must come into the NRP-2 via ATM (PPPoEoA)

- PPPoE sessions are terminated directly on the NRP-2; no L2TP tunneling is involved
- PPPoE session traffic is routed out the GE interface on the same NRP-2

Cisco recommends 512 MB memory on the NRP-2 to support 8000 sessions. Session counts for PPPoE tunneled, PPPoA terminated or tunneled, RBE, and RFC 1483 IP routed remain at 4000 sessions on the NRP-2 for Release 12.1(5)DC.

CEF Switching for Routed Bridge Encapsulation

The CEF Switching for Routed Bridge Encapsulation feature adds Cisco Express Forwarding (CEF) switching support to ATM routed bridge encapsulation (RBE). Prior to this release, ATM RBE supported only fast switching and process switching. The ATM RBE feature is used to route IP over bridged RFC 1483 Ethernet traffic from a stub-bridged LAN.

DHCP Option 82 Support for Routed Bridge Encapsulation

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

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

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

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

HTTP Redirect (for the Service Selection Gateway)

The Hypertext Transfer Protocol (HTTP) Redirect feature works in conjunction with the Cisco Service Selection Dashboard (SSD) to implement captive portals. If a user has not logged in and sends packets upstream to a configurable group of TCP ports, SSG sends those packets to a captive portal group (one or more servers). The SSG handles the incoming packets in a suitable manner, such as returning a login page.

The group of captive portals consists of one or more SSDs, which may or may not be arranged in order of priority. The SSG will redirect packets to the captive portal groups on a round-robin basis.

The HTTP Redirect feature provides a means for user authentication without requiring the user to know about the dashboard URL. It enables service providers to implement captive portals, own the user experience, advertise value-added services, and build a brand experience.



Note

The HTTP Redirect feature requires Release 3.0(1) of the SSD, which is scheduled to ship in June.

**Note**

In Cisco IOS Release 12.1(5)DC, the HTTP Redirect feature is not supported for subscribers connecting to SSG using PPP and RBE.

The following new CLI commands are introduced for the HTTP Redirect feature:

Defining a captive portal group:

ssg http-redirect group <groupname> **server** <ip address> <port>

Adding a TCP port to a portal group:

ssg http-redirect port <incoming destination port number> **group** <groupname>

Adding a destination service address to a portal group:

ssg http-redirect bind <service name> **group** <groupname>

Setting a default group for unauthorized user redirection:

ssg http-redirect unauthorized-user group <groupname>

Setting the frequency of loading requests to send to servers in a group:

ssg http-redirect group <groupname> **poll-frequency** <frequency>

Setting the time before a server is declared inactive:

ssg http-redirect group <groupname> **retry-count** <count>

Displaying captive portal groups:

show ssg http-redirect [<name>]

Displaying debug HTTP redirect information:

debug ssg http-redirect [packet |server]

For more information about the HTTP Redirect feature, see the *Node Route Processor—Service Selection Gateway Enhancements V* feature module.

IP Overlapping Address Pools (OAP) (NRP-1 only)

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

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

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

The following CLI commands have been revised for the IP OAP feature:

Defining a pool:

This existing **ip local pool** syntax is extended to:

ip local pool <pool-name> <start-IP> [<end-IP>] [group <group-name>] [cache-size <size>]

Displaying a pool:

This existing **show** command syntax is extended to:

```
show ip local pool [[group <group-name>] | [ <poolname> ]]
```

For more information about the IP OAP feature, see the *Overlapping IP Address Pools* feature module.



Note

Future releases may support this feature for the NRP-2.

NetFlow Switching with RFC 1483 (NRP-1 only)

NetFlow switching is now supported on the Cisco 6400 NRP-1 when used with RFC 1483 routed PVCs in MPLS VPNs. The netflow records only record data flowing into the MPLS VPN. For more information about NetFlow switching, see the *NetFlow Switching* chapter of the *Cisco IOS Switching Services Configuration Guide, Release 12.1*. For examples of RFC 1483 routed PVCs in MPLS VPNs, see the *Configuring Multiprotocol Label Switching on the Cisco 6400 UAC* configuration note.



Note

Future releases may support this feature for the NRP-2.

New NRP-2 features (Feature synchronization)

As of Cisco IOS Release 12.1(5)DC, the following features, which were already supported for the NRP-1, are also supported for the NRP-2:

- GRE CEF
- GRE tunnel on packet interface
- Per-VC Error Display
- PPPoA/oE autosense SNAP
- PPPoE Fast Switching for Multicast
- SSG local forwarding
- SSG with GRE
- VPI/VCI in RADIUS Request and RADIUS Accounting for PPPoA
- VPI/VCI in RADIUS Request and RADIUS Accounting for PPPoE

Open Garden (for the Service Selection Gateway)

An Open Garden is one or more domains that may be accessed without user authentication. This differs from a “Walled Garden”. A “Walled Garden” refers to a collection of websites, or networks in general, that a user can access after providing minimal authentication information.

The Open Garden enhancement enables a list of up to 100 domains to be associated with the default network. If a subscriber creates a DNS request for one of those domain names, the DNS request will be resolved by the SSG to the default network. This ensures that a subscriber will be able to access the Service Selection Dashboard, which typically resides on the management network with a private address, even when the subscriber is assigned a public DNS server.

With the Open Garden enhancement, a subscriber can access a limited number of websites without logging into the network. The administrator can configure which sites a non-authenticated user is allowed to access.

The following new CLI commands are introduced for the Open Garden feature:

Specifying each of the Open Garden networks:

local profile <[name]>

Local profile attributes “R”, “O”, and “D”, where networks and domain names lists can be configured for each Open Garden network:

“R” Open Garden Network

“O” Domain Names List

“D” DNS IP address in Open Garden network.

Entering a profile configuration mode and configuring a local RADIUS service profile:

Router(config)# **local-profile** profilename

Configuring an attribute in a local RADIUS service profile:

Router(config-prof)# **attr radius-attribute-id** [vendor-id] [cisco-vs-a-type] attribute-value

Adding this newly created profile to the Open Garden list:

ssg open-garden <service profile name>

Displaying all the Open Garden networks configured:

sh ssg open-garden

For more information about the Open Garden enhancement, see the *Node Route Processor—Service Selection Gateway Enhancements V* feature module.

RADIUS Attribute 4 and Format d—Introduction of a New Command

When using RADIUS attribute 4 and “format d” in a VPI/VCI configuration or in a SSG configuration, the new command **radius-server attribute 4 nrp** allows the default-selected IP address to be changed. This command can only be enabled if “format d” is already configured.

Table 3 shows how RADIUS global configuration commands can be combined to select an IP address.

Table 3 RADIUS Global Configuration Commands and Selected IP Addresses

Global Configuration Commands			Selected IP Address
ip radius source-interface <int x>	radius-server attribute nas-port format d	radius-server attribute 4 nrp	
Enabled			NRP IP address ¹
	Enabled		NSP IP address
Enabled	Enabled		NSP IP address

Table 3 RADIUS Global Configuration Commands and Selected IP Addresses (continued)

Global Configuration Commands			Selected IP Address
ip radius source-interface <int x>	radius-server attribute nas-port format d	radius-server attribute 4 nrp	
Enabled	Enabled	Enabled	NRP IP address ¹
	Enabled	Enabled	NRP best-select IP address ²

1. NRP IP address of <int x>
2. Automatic choice, 1st choice is loopback, etc.

New Hardware Features Supported in Release 12.1(4)DC2

The following new hardware features are supported by the Cisco 6400 NRP for Cisco IOS Release 12.1(4)DC2.

Node Route Processor 2 (NRP-2)

The second-generation node route processor (NRP-2) for the Cisco 6400 platform allows aggregation and termination of large numbers of broadband subscribers while supporting Layer 3 and integrated high-touch services such as authentication, policy routing, and Network Address Translation (NAT). The Cisco 6400 receives subscribers over OC-3, OC-12, or DS-3 interfaces on node line cards (NLCs). The node switch processor (NSP) switches incoming virtual circuits (VCs) or virtual paths (VPs) to the appropriate NRP-2. The NRP-2 aggregates and terminates the incoming virtual circuits (VCs), offering extended services based on user and service profiles through the Service Selection Gateway (SSG).

Benefits of the NRP-2

In comparison with the NRP-1, the NRP-2 provides the following benefits:

Increased Session Scalability

The NRP-2 increases the session capacity of the Cisco 6400, providing a dramatic reduction in cost per subscriber. [Table 5 on page 23](#) shows the number of sessions and tunnels supported by the NRP-2 in Cisco IOS Release 12.1(4)DC2 and subsequent releases.

Increased Bandwidth

The NRP-2 supports a 622-Mbps ATM interface to the backplane and a Gigabit Ethernet (GE) packet interface on the faceplate.

Dual Processors

The NRP-2 hardware includes two processor subsystems. In Cisco IOS Release 12.1(4)DC2, only one of the processors is used. In future software releases, the second processor will be used to provide increased session scalability.

Integrated System Management

Configuration storage, console traffic, and network management traffic are now controlled by the existing NSP, providing a more manageable and integrated platform. You can use a single console port on the NSP to access the console lines of all NRP-2s in the Cisco 6400 chassis and use a single management Ethernet interface on the NSP to monitor all NRP-2s in the system.

Backward Compatibility

The NRP-2 can be deployed in a Cisco 6400 chassis with existing modules, including the first-generation NRP-1. This enables you to increase your network capacity without replacing the chassis.



Note

In redundant configurations, NRPs must be paired with NRPs of the same type (NRP-1 with NRP-1, NRP-2 with NRP-2). However, note that Cisco IOS Release 12.1(4)DC2 and subsequent releases do not support redundancy on the NRP-2. Future software releases may introduce redundancy support on the NRP-2.

Modular Design

The modular nature of the NRP-2 allows you to upgrade as your subscriber base grows. As the demand for services rises, you can add NRP-2 modules to the Cisco 6400 to provide increased session and bandwidth support.

Differences Between the NRP-1 and NRP-2

Table 4 shows the major differences between the NRP-1 and NRP-2.

Table 4 Differences Between NRP-1 and NRP-2

Characteristic	NRP-1	NRP-2
Session scalability	Hardware supports as many as 2000 sessions per NRP-1.	Hardware supports as many as 16,000 sessions per NRP-2
Physical interfaces	Faceplate interfaces: <ul style="list-style-type: none"> • Console port • Auxiliary port • Ethernet port • Fast Ethernet port Backplane interfaces: <ul style="list-style-type: none"> • 155-Mbps ATM interface • Backplane Ethernet (BPE) 	Faceplate interfaces: <ul style="list-style-type: none"> • Gigabit Ethernet interface¹ Backplane interfaces: <ul style="list-style-type: none"> • 622-Mbps ATM interface • PAM² mailbox serial interface³
Location of software images, configurations, and crash information	NRP-1 memory (built-in or internal Flash)	PCMCIA ⁴ disk on NSP
Message logging	Messages are logged on the NRP-1 as local messages.	NRP-2 messages are logged on both the NSP and NRP-2. NRP-2 messages on the NSP include the NRP-2 slot number.
Console line access	Direct external connection to NRP-1 console port or auxiliary port	Indirect external connection via the NSP. NSP contains a virtual communication server to access the NRP-2 console.

Table 4 Differences Between NRP-1 and NRP-2 (continued)

Characteristic	NRP-1	NRP-2
ROMMON ⁵	ROMMON not upgradable; NRP-1 ROM state information stored locally on NRP-1	ROMMON is upgradable; NRP-2 ROM state information is stored on the NSP PCMCIA disk.
SNMP ⁶	Standard SNMP services	Standard SNMP services, or can use the NSP as the proxy forwarder
LED display	None	On faceplate

1. The GE interface is not supported in Cisco IOS Release 12.1(4)DC2. Support for the GE interface is introduced in Cisco IOS Release 12.1(5)DC.
2. PAM = Pulse amplitude modulation
3. The PAM mailbox serial interface is used for internal system communication. Do not attempt to configure serial interfaces on the Cisco 6400.
4. PCMCIA = Personal Computer Memory Card International Association
5. ROMMON = ROM Monitor
6. SNMP = Simple Network Management Protocol

More Information about the NRP-2

For more information about the NRP-2, see the *NRP-2* feature module.

New Software Features Supported in Releases 12.1(4)DC2

The following new software features are supported by the Cisco 6400 NRP for Cisco IOS Release 12.1(4)DC2.

ATM PVC Range and RBE Subinterface Grouping by PVC Range

In a digital-subscriber line (DSL) environment, many applications require the configuration of a large number of ATM permanent virtual circuits (PVCs). The ATM PVC Range and routed bridge encapsulation (RBE) Subinterface Grouping feature enables you to group a number of PVCs together into a PVC range in order to configure them all at once.

For applications that use multipoint subinterfaces, such as PPP over Ethernet and PPP over ATM, the PVC range is on a single multipoint subinterface. For applications that use point-to-point subinterfaces, such as RBE, a point-to-point subinterface is created for each PVC in the range.

Configuring many PVCs and subinterfaces at once saves time for the user and the parser, and conserves NVRAM space.

A PVC range is defined by two virtual path identifier (VPI)/virtual channel identifier (VCI) pairs. The two VPIs define a VPI range, and the two VCIs define a VCI range. The number of PVCs in the PVC range equals the VPI range multiplied by the VCI range.

Once the PVC range is defined, you can configure the range by using the existing Interface-ATM-VC configuration commands that are also supported in PVC range configuration mode. The **shutdown** PVC range command can be used to deactivate the range without deleting the configuration.

The ATM PVC Range and RBE Subinterface Grouping feature also introduces the *pvc-in-range* command, which allows you to explicitly configure an individual PVC within the defined range of PVCs on a multipoint subinterface. The **shutdown** PVC-in-range command allows you to deactivate an individual PVC within a range.

ATM PVC Range only supports multipoint ATM subinterfaces. You cannot configure individual PVCs within a PVC range on point-to-point subinterfaces. You must remove the individual PVC configurations from the configuration file to take advantage of the PVC range. If multiple configurations remain in the file, these configurations will override the PVC range commands.

For more information about this feature, see the *ATM PVC Range and Routed Bridge Encapsulation Subinterface Grouping* feature module.

**Note**

This feature is supported for both the NRP-1 and NRP-2.

New Hardware Features Supported in Release 12.1(3)DC1

There are no new hardware features for the Cisco 6400 NRP supported in Cisco IOS Release 12.1(3)DC1.

New Software Features Supported in Release 12.1(3)DC1

The following new software features are supported by the Cisco 6400 NRP for Cisco IOS Release 12.1(3)DC1.

IPCP Subnet Mask Support Enhancements

IP Control Protocol (IPCP) subnet mask support allows customer premise equipment (CPE) to connect to the Cisco 6400 NRP and obtain an IP address and subnet mask range that it can use to populate its Dynamic Host Configuration Protocol (DHCP) server database. However, the software default setting does not allow subnet negotiations.

To enable IPCP subnet mask support, issue the **ppp ipcp mask** CLI command. In addition, a value must be specified for the **Framed-IP-Netmask** attribute (Internet Engineering Task Force [IETF] RADIUS attribute 9) in the RADIUS user profile.

The Cisco 6400 NRP brings up PPP sessions with the CPE and authenticates each CPE as a separate user. The Cisco 6400 NRP adds a static route for the IP address with the subnet mask specified. If the subnet mask is specified in the user profile, the Cisco 6400 NRP passes the IP netmask value and the IP address to the CPE during IPCP negotiation. The CPE uses the subnet mask to calculate an IP address pool from which IP addresses are assigned to PCs using the access link.

For more information about the IPCP subnet mask support feature, see the *PCP Subnet Mask Support Enhancements* feature module.

**Note**

The IPCP subnet mask support feature was introduced in Cisco IOS Release 12.0(5)DC.

Multilink PPP

Multilink Point-to-Point Protocol (PPP), referred to as MLPPP or MLP, is now supported on the Cisco 6400 NRP. MLP provides a method for spreading traffic across multiple physical WAN links while providing packet fragmentation and reassembly, proper sequencing, multivendor interoperability, and load balancing on inbound and outbound traffic. MLP provides bandwidth on demand and reduces transmission latency across WAN links.

For information about configuring MLP, see the chapter *Configuring Media-Independent PPP and Multilink PPP in the PPP Configuration* section of the *Cisco IOS Dial Services Configuration Guide: Terminal Services*.

L2TP LAC CEF Switching

Cisco express forwarding (CEF) is now supported on the Cisco 6400 NRP configured as an L2TP access concentrator (LAC).

For more information about CEF, see the chapter “Cisco Express Forwarding” in the *Cisco IOS Switching Services Configuration Guide*. For more information about L2TP, see the *Layer2Tunnel Protocol Scalability Enhancements* feature module.

Single-Host Logon

Single-Host Logon is an enhancement to the Node Route Processor—Service Selection Gateway (NRP-SSG). Single-Host Logon combines the PPP session logon and NRP-SSG host logon steps into one.

For more information, see the *Node Route Processor-Service Selection Gateway Enhancements IV* feature module.



Note

For NRP-Service Selection Gateway (SSG) users, Cisco IOS Release 12.1(5)DC works with the Cisco Service Selection Dashboard (SSD) version 2.5(1) that supports the Single-Host Logon feature.



Note

The SSG allows subscribers to log on to services and reach the service network, even when there is no static service binding on the SSG, nor a dynamic binding using a Next Hop Gateway (NHG) table.

Per VC Error Display

The command **show controllers atm** of the command language interface (CLI) was modified to allow the user to:

- enable the output of cyclic redundancy check (CRC) error counts on a per-virtual circuit (VC) basis,
- display only segmentation and reassembly (SAR) controller information as the default output,
- control the output with new options, including error counters on a per-VC basis.

For more information about this feature, see the *Per VC Error Display* feature module.

RADIUS Attribute 8 (Framed-IP-Address) in Access Requests

The RADIUS Attribute 8 (Framed-IP-Address) in Access Requests feature makes it possible for a network access server to provide the RADIUS server with a hint of the user IP address in advance of user authentication. An application can be run on the RADIUS server to use this hint and build a table (map) of user names and addresses. Using the mapping information, service applications can begin preparing user login information to have available upon successful user authentication.

For more information about this feature, see the *RADIUS Attribute 8 (Framed-IP-Address) in Access Requests* feature module.

Service Selection Gateway (SSG) Proxy RADIUS Enhancements

The Cisco 6400 NRP-SSG feature was first released in Cisco IOS Releases 12.0(3)DC, while enhancements were added in subsequent releases. Releases 12.1(3)DC1 introduces the following Proxy RADIUS Enhancements:

- Service-Defined Cookie—A configurable vendor-specific attribute (VSA) that allows user-defined information to be included in the RADIUS authentication and accounting requests.
- Full Username RADIUS Attribute—Enables usage of the full username (user@service) in the RADIUS authentication and accounting requests.

For more information about these enhancements, see the *Node Route Processor-Service Selection Gateway Enhancements IV* feature module.

New Hardware Features Supported in Release 12.1(1)DC1

There are no new hardware features for the Cisco 6400 NRP supported in Cisco IOS Release 12.1(1)DC1.

New Software Features in Release 12.1(1)DC1

The following new software features are supported by the Cisco 6400 NRP for Cisco IOS Release 12.1(1)DC1.

Cisco Express Forwarding

CEF switching is now supported for PPP over ATM (PPPoA), generic routing encapsulation (GRE), and Network Address Translation (NAT).

Dynamic Host Configuration Protocol Relay for Unnumbered Interfaces Using ATM RBE

Dynamic Host Configuration Protocol (DHCP) Relay now supports unnumbered interfaces using ATM route bridge encapsulation (RBE). DHCP Relay automatically adds a static host route specifying the unnumbered interface as the outbound interface.

DHCP Relay now also can use the **ip dhcp database** global configuration command. This optional command allows the DHCP Relay to save route information to a TFTP, FTP, or RCP server for recovery after reloads.

For more information about DHCP, see “Configuring DHCP” in the *Cisco IOS IP and IP Routing Configuration Guide* and “DHCP Commands” in the *Cisco IOS IP and IP Routing Command Reference*. For more information about the ATM RBE feature, see the *ATM Routed Bridge Encaps* feature module.

Session Scalability Enhancements

The following enhancements provide better session stability:

- Increased input and output hold-queue limits
- Limiting the number of simultaneous link control protocol session initiations
- Limiting the load metric

For more information, see the *Session Scalability Enhancements II* feature module.

L2TP Tunnel Management Enhancements

The L2TP tunnel management enhancements include the following features:

- Tunnel Sharing—Enables sessions authorized with different domains to share the same tunnel
- Sessions per Tunnel Limiting—Enables the **initiate-to** command to limit the number of sessions per L2TP tunnel

For more information, see the *L2TP Tunnel Management Enhancements* feature module

L2TP Tunnel Service Authorization Enhancements

These enhancements enable the L2TP access concentrator (LAC) to conduct static or dynamic tunnel service authorization. A static domain name can be configured on the ATM permanent virtual circuit (PVC) port to override the domain name supplied by the client. If a static domain name is not configured, the LAC conducts dynamic tunnel service authorization, which now includes two steps:

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

For more information, see the *L2TP Tunnel Service Authorization Enhancements* feature module.

L2TP Tunnel Switching

This feature enables the Cisco 6400 NRP to terminate tunnels from LACs and forward the sessions through new L2TP tunnels selected independently of the client-supplied domains. The NRP as a tunnel switch performs virtual private dial-up network (VPDN) tunnel authorization based on the ingress tunnel names that are mapped to specified LTP Network Servers (LNSs).

For more information, see the *L2TP Tunnel Switching* feature module.

Node Route Processor-Service Selection Gateway—Local Forwarding

This feature includes the Local Forwarding enhancement to the Node Route Processor—Service Selection Gateway (NRP-SSG). Local Forwarding enables NRP-SSG to forward packets locally.

For more information, see the *Node Route Processor—Service Selection Gateway Enhancements III* feature module.

Segmentation and Reassembly Buffer Management Enhancements for the NRP-1

This feature includes the following enhancements to segmentation and reassembly (SAR) buffer management:

- Reduced segmentation buffer size
- Increased input/output memory size
- Reserved segmentation buffer slot for high-priority packets

For more information, see the *Segmentation and Reassembly Buffer Management Enhancements* feature module.

PPP Autosense

The PPP Autosense feature enables the network access server to:

- Distinguish between incoming PPPoA and PPP over Ethernet (PPPoE) sessions with Subnetwork Access Protocol (SNAP) encapsulation
- Allocate resources on demand for both PPP types.

For more information, see the *PPP Autosense* feature module.

PPP over Ethernet (PPPoE) Fast Switching for Multicast

PPPoE now supports fast switching for multicast in addition to Cisco express forwarding (CEF).

VPI/VCI Identification in RADIUS Requests

This feature enables the RADIUS VC Logging [Cisco IOS Release 12.0(5)DC] feature to support PPPoE. With RADIUS VC Logging enabled, the RADIUS network access server port field is extended and modified to carry VPI/VCI information. This information is logged in:

- RADIUS accounting record created at session startup
- RADIUS authentication requests

For more information, see the *RADIUS VC Logging* feature module.

Limitations and Restrictions

This section describes the following limitations:

- Cutting and Pasting through the NRP-2 Console Port
- Maximum Transmission Unit
- VPI and VCI Limitations

Cutting and Pasting through the NRP-2 Console Port

The NRP-2 does not support the cutting and pasting of configurations through the console port. Doing so might cause the NRP-2 to pause indefinitely.

Maximum Transmission Unit

The maximum transmission unit (MTU) of the NRP-2 ATM interface to the backplane is 1900 bytes. Any incoming packet larger than 1900 bytes is dropped by the NRP-2. To make sure that no incoming packets are larger than the NRP-2 MTU, see the section *Matching the MTU Size of the NRP-2 and Its Network Neighbors (Optional)* in the *NRP-2* feature module.

Traffic Shaping on the NRP-2

In Cisco IOS Release 12.1(5) DC2, the NRP-2 does not support available bit rate (ABR), unspecified bit rate (UBR), or variable bit rate (VBR) traffic shaping. Future releases might support traffic shaping on the NRP-2.

VPI and VCI Limitations

VPI and VCI values on the NRP-2 must share 14 bits. By default, VPI values are limited to 4 bits (0-15), and VCI values are limited to 10 bits (0-1023). You can change the VPI and VCI ranges, but together the VPI and VCI values cannot exceed 14 bits. To change the allowed VPI and VCI values, see the *Modifying VPI and VCI Ranges (Optional)* section in the *NRP-2* feature module.

Important Notes

Service Selection Gateway—Change in Service Object Behavior

Up to Cisco IOS Release 12.1(5) DC2, when there was no user who used a service, the Service Selection Gateway service object was removed automatically when the last user logged off the service.

As of Cisco IOS Release 12.1(5) DC2, the service object stays in the system after all users who have used the service have logged off. The same service object will be reused when a user logs on to the service again. If the administrator knows that the service has become obsolete, the administrator can remove the service object through the CLI command **clear ssg service** *<service name>*.

Session and Tunnel Scalability

Cisco IOS Release 12.1(5) DC2 supports the number of sessions and tunnels shown in [Table 5](#). While using NRP-SSG, Cisco IOS Release 12.1(5) DC2 supports the number of sessions and tunnels shown in [Table 6](#).

Table 5 Session and Tunnel Scalability in Cisco IOS Release 12.1(5) DC2

Protocol	NRP-1		NRP-2	
	Number of Supported Sessions	Number of Supported Tunnels	Number of Supported Sessions	Number of Supported Tunnels
L2TP PPPoA	up to 1700	up to 300	up to 4000	up to 1000
L2TP PPPoE	up to 2000	up to 300	up to 4000	up to 1000
L2TP Tunnel Switch PPPoA	up to 940	up to 50 Ingress up to 10 Egress	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	up to 940	up to 50 Ingress up to 10 Egress
PPPoA	up to 2000	—	up to 4000	—
PPPoE	up to 2000	—	up to 8000	—
PPP Autosense	up to 2000	—	up to 4000	—
RBE	up to 2000	—	up to 4000	—
RFC 1483 IP Routed	up to 2000	—	up to 4000	—

Table 6 NRP-SSG Session and Tunnel Scalability in Cisco IOS Release 12.1(5) DC2

Protocol with NRP-SSG	NRP-1		NRP-2	
	Number of Supported Sessions	Number of Supported Tunnels	Number of Supported Sessions	Number of Supported Tunnels
L2TP PPPoA	up to 700	up to 100	up to 2000	up to 1000
L2TP PPPoE	up to 700	up to 100	up to 1500	up to 1000
PPPoA	up to 2000	—	up to 4000	—
PPPoE	up to 2000	—	up to 4000	—
RBE	up to 2000	—	up to 4000	—
RFC 1483 IP Routed	up to 2000	—	up to 4000	—



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.



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

Session Scalability Commands

This section provides commands that can be applied to achieve the session counts listed in [Table 5](#) and [Table 6](#).

[Table 7](#) and [Table 8](#) list commands for which Cisco recommends a particular setting in Cisco IOS Release 12.1(5) DC2. [Table 9](#) lists additional commands that might be useful to achieve high session counts, but for which no recommended settings are provided; the setting of these commands depends on the user’s environment and configuration.

For additional information, refer to the *Layer 2 Tunnel Protocol Scalability Enhancements* feature module and the *Session Scalability Enhancements* feature module.

L2TP Session Scalability Commands with Recommended Settings for Both the NRP-1 and NRP-2

[Table 7](#) lists L2TP session scalability commands with recommended settings that apply to both the NRP-1 and NRP-2 in Cisco IOS Release 12.1(5) DC2.

Table 7 L2TP Session Scalability Commands with Recommended Settings for the NRP-1 and NRP-2

Configuration Task and Commands	Guidelines
Modifying the PPP Max Configure: NRP(config)# ppp max-configure <i>number</i>	1. Purpose Specifies the number of Configure Requests.
	2. Symptoms Use when a large number of connections flap ¹ .
	3. Recommended Settings To achieve a large number of sessions, Cisco recommends a setting of 225 (that is, the value for <i>number</i>) on the NRP-1 and NRP-2.
Precloning Virtual Access Interfaces: NRP(config)# virtual-template <i>template-number</i> preclone <i>number</i>	1. Purpose Specifies the number of virtual access interfaces to be created and cloned from a specific virtual template.
	2. Symptoms Use to reduce the load on the system during call setup.
	3. Recommended Settings The recommended setting depend on the number of sessions that need to be configured. For example, to configure 2000 sessions on the NRP-1, enter a value of 2000 for <i>number</i> ; to configure 4000 sessions on the NRP-2, enter a value of 4000 for <i>number</i> .

1. Flapping = Routing problem where an advertised route between two nodes alternates (flaps) back and forth between two paths due to a network problem that causes intermittent interface failures.

L2TP Session Scalability Commands with Recommended Settings for the NRP-2

Table 8 lists L2TP session scalability commands with recommended settings that apply to the NRP-2 in Cisco IOS Release 12.1(5) DC2.

Table 8 L2TP Session Scalability Commands With Recommended Settings for the NRP-2

Configuration Task and Commands	Guidelines
Increasing the Input Hold-Queue Limit: <ul style="list-style-type: none"> • NRP(config)# interface atm <i>slot/subslot/port</i> • NRP(config-if)# hold-queue <i>length in</i> 	1. Purpose Specifies the maximum number of packets in the input hold-queue.
	2. Symptoms Use when the show interfaces EXEC command reveals an excessive number of discarded packets because of input hold-queue overflows.
	3. Recommended Settings To accommodate more incoming control messages in the queue, set the maximum number of packets to a high value: NRP-2: 1000 packets or more

Table 8 L2TP Session Scalability Commands With Recommended Settings for the NRP-2 (continued)

Configuration Task and Commands	Guidelines
Increasing the Output Hold-Queue Limit: <ul style="list-style-type: none"> NRP(config)# interface atm slot/subslot/port NRP(config-if)# hold-queue length out 	<p>1. Purpose Specifies the maximum number of packets in the output hold-queue.</p> <p>2. Symptoms Use when the show interfaces EXEC command reveals an excessive number of discarded packets because of output hold-queue overflows.</p> <p>3. Recommended Settings To accommodate more outgoing control messages in the queue, set the maximum number of packets to a high value: NRP-2: 1000 packets or more</p>

Additional L2TP Session Scalability Commands

Table 9 lists additional commands that might be useful to achieve the session counts listed in Table 5 and Table 6, but for which no recommended settings are provided; the setting of these commands depends on the user’s configuration and environment.

Table 9 Additional L2TP Session Scalability Commands Without Recommended Settings

Configuration Task and Commands	Guidelines
Limiting the Number of LCP Session Initiations: NRP(config)# lcp max-session-starts number	<p>1. Purpose Specifies the maximum number of simultaneous LCP sessions to be negotiated.</p> <p>2. Symptoms Use when a large number of parallel LCP sessions causes many sessions to timeout and retry, which can result in a chain reaction of LCP session negotiations and excessive session recovery times.</p> <p>3. Settings Information To limit the number of simultaneous LCP session initiations, set the value for <i>number</i> between 100 and 3000.</p>
Limiting the Load Metric: NRP(config)# lcp max-load-metric number	<p>1. Purpose Specifies the maximum load metric based on the length of the PPP manager process input queue.</p> <p>2. Symptoms Use to shorten the session recovery time after a link dropout.</p> <p>3. Settings Information The nominal value for <i>number</i> depends on many factors. Cisco recommends that you start with 100. Try several values and select the one that results in the shortest session-recovery time after a link dropout.</p>

Table 9 Additional L2TP Session Scalability Commands Without Recommended Settings (continued)

Configuration Task and Commands	Guidelines
Modifying the PPP Authentication Timeout: <ul style="list-style-type: none"> NRP(config)# interface virtual-template <i>number</i> NRP (config-if)# ppp timeout authentication <i>seconds</i> 	<p>1. Purpose Specifies the PPP authentication timeout.</p> <p>2. Symptoms Use when the number of stable sessions is low because the waiting time for a response from the remote peer is too short, resulting in a PAP¹ authentication request, CHAP² challenge, or CHAP response being retransmitted.</p> <p>3. Settings Information The default PPP authentication timeout is 10 seconds. On the NRP-2, to increase the PPP authentication timeout, start with 15 seconds. Try several numbers and select the one that results in the highest number of stable sessions. (The maximum number is 255 seconds.)</p>
Modifying the PPP Retry Timeout: <ul style="list-style-type: none"> NRP(config)# interface virtual-template <i>number</i> NRP(config-if)# ppp timeout retry <i>seconds</i> 	<p>1. Purpose Specifies the PPP retry timeout.</p> <p>2. Symptoms Use when the number of stable sessions is low because the waiting time for a response from the remote peer is too short, resulting in a configuration request or connection-termination request being retransmitted.</p> <p>3. Settings Information The default PPP retry timeout is 2 seconds. On the NRP-2, to increase the PPP retry timeout, start with 15 seconds. Try several numbers and select the one that results in the highest number of stable sessions. (The maximum number is 255 seconds.)</p>
Setting the Number of Retransmission Attempts: <ul style="list-style-type: none"> NRP(config)# vpdn-group <i>number</i> NRP(config-vpdn)# l2tp tunnel retransmit retries <i>value</i> 	<p>1. Purpose Specifies the number of retransmission attempts per selected VPDN group.</p> <p>2. Symptoms Use when the number of retransmission attempts is insufficient.</p> <p>3. Settings Information The default number of L2TP tunnel control channel retransmission attempts is 10.</p>
Setting the Minimum and Maximum Retransmission Timeouts: <ul style="list-style-type: none"> NRP(config)# vpdn-group <i>number</i> NRP(config-vpdn)# l2tp tunnel retransmit timeout min <i>seconds</i> NRP(config-vpdn)# l2tp tunnel retransmit timeout max <i>seconds</i> 	<p>1. Purpose Specifies the minimum or maximum timeout for retransmissions on a selected VPDN group.</p> <p>2. Symptoms Use when the timeout for retransmissions is too short or too long. To determine the best minimum and maximum timeouts for a given topology, use the privileged EXEC command show vpdn tunnel all and check the displayed retransmit time distribution.</p> <p>3. Settings Information Control channel retransmissions follow an exponential backoff, starting at the minimum retransmission timeout, and ending at the maximum retransmission timeout. The maximum timeout can be set to up to 8 seconds.</p>

Table 9 Additional L2TP Session Scalability Commands Without Recommended Settings (continued)

Configuration Task and Commands	Guidelines
Setting the Local Control Channel Receive Window Size: <ul style="list-style-type: none"> NRP(config)# vpdn-group <i>number</i> NRP(config-vpdn)# l2tp tunnel receive-window <i>packets</i> NRP(config-vpdn)# exit NRP(config)# end NRP# clear vpdn tunnel l2tp <i>remote-name local-name</i> 	1. Purpose Specifies the size of the advertised receive window per selected VPDN group, clears all sessions, and drops the tunnel.
	2. Symptoms Use when the L2TP control channel sends requests too slowly.
	3. Settings Information The default local receive window size (RWS) is 3000 packets.
Setting the L2TP Tunnel Timeout: <ul style="list-style-type: none"> NRP(config)# vpdn-group <i>number</i> NRP(config-vpdn)# l2tp tunnel no-session-timeout <i>seconds</i> 	1. Purpose Specifies the tunnel timeout length per selected VPDN group.
	2. Symptoms Use when a tunnel timeout is too short. For example, after all of its sessions are gone and you expect sessions to come back immediately, you might want to keep the tunnel open.
	3. Settings Information The default tunnel timeout is 10 seconds for an LNS and 15 seconds for an LAC.

1. PAP = Password Authentication Protocol
2. CHAP = Challenge Handshake Authentication Protocol

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 12.1 and Cisco IOS Release 12.1 T are also in Cisco IOS Release 12.1(5) DC2.

For information on caveats in Cisco IOS Release 12.1, see *Caveats for Cisco IOS Release 12.1*.

For information on caveats in Cisco IOS Release 12.1 T, see the *Caveats for Cisco IOS Release 12.1 T*, which lists severity 1 and 2 caveats and select severity 3 caveats and is located on Cisco.com and the Documentation CD-ROM.



Note

Cisco IOS Release 12.1(5) DC2 is in synchronization with Cisco IOS Release 12.1(5)T4.

Caveat numbers and brief descriptions are listed in [Table 10](#). For details about a particular caveat, go to Bug Toolkit at:

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

To access this location, you must have an account on Cisco.com. For information about how to obtain an account, go to the “[Cisco Feature Navigator](#)” section on [page 50](#).

**Note**

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

Open Caveats—Cisco IOS Release 12.1(1) DC2

There are no open caveats specific to Cisco IOS Release 12.1(1) DC2 that require documentation in the release notes.

Resolved Caveats—Cisco IOS Release 12.1(1) DC2

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(1) DC2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdw65903

An error can occur with management protocol processing. Please use the following URL for further information:

<http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903>

Open Caveats—Release 12.1(5)DC1

There are no open caveates in Cisco IOS Release 12.1(5)DC1.

Resolved Caveats—Release 12.1(5)DC1

All the caveats listed in [Table 10](#) are closed or resolved in Cisco IOS Release 12.1(5)DC1. This table lists only severity 1 and 2 caveats and select severity 3 caveats.

Table 10 *Closed or Resolved Caveats for Release 12.1(5)DC1*

Caveat ID Number	Description
CSCds15443	TAG TDP stops running after reboot on ethernet interface
CSCds30806	OSPF:scanner displays error messages for Type3 LSAs
CSCDs73113	DHCP packets are not forwarded on second configured RBE interface
CSCdt02925	Relay gets bus error for relay_unnumber_db when C cant get reply
CSCdt31521	TFIB:TFIB tag-rewrite memory leak
CSCdt34231	NRP1FastEthernet0/0/0 flaps when adding/removing subinterfaces
CSCdt47730	OSPF and XtagATM interface issues on NRP when NSP reloads
CSCdt51547	Packet drop with ip verify unicast reverse-path
CSCdt65960	For NRP2, access-list not working on VTY when telnet GigEther port
CSCdt69283	Relay agent is not renewing the binding using dhcp unnumbered.

Table 10 Closed or Resolved Caveats for Release 12.1(5)DC1

Caveat ID Number	Description
CSCdt69881	Memory leak, memory allocation failure
CSCdt85227	A watchdog forced crash - meaning, ExtractQNameAsDomainName
CSCdt92513	Bus Error with long L2TP Tunnel-Server-Auth-ID (50/60 chars)
CSCdt93857	Memory leak
CSCdt96357	Radius attribute 4 NRP configuration disappears upon reload of NRP
CSCdu10108	Service name not inherited from VC Class

Open Caveats—Release 12.1(5)DC

This section describes possibly unexpected behavior by Cisco IOS Release 12.1(5)DC. This section describes severity 1 and 2, and selected severity 3 and 4 caveats.

Caveats that Apply to Both the NRP-1 and NRP-2

The following open caveats apply to both the NRP-1 and NRP-2.

- CSCdp19647

After all NRP-SSG users log off a specific service, the service object is cleared, but the subblock associated with the interface is not reset. As a result, all traffic from the interface is still treated by NRP-SSG as downstream traffic.

Workaround (do one of the following):

 - Enter the **no ssg bind direction uplink** global configuration command for the affected interface
 - Reload the NRP
- CSCdp29451

Changing service binding while using the service might cause an inconsistency in the service binding table and break the NRP-SSG data path forwarding table.

Workaround: Avoid changing service binding while the service is in use.
- CSCdp59354

Traffic coming from a Fast Ethernet (FE) interface on an NRP with Inter-Switch Link (ISL) encapsulation, forwarded out of an ATM route bridge encapsulation (RBE) interface, might not be fast-switched but process-switched when you use the **bridge irb** global configuration command on the NRP.

Workaround: Remove the **bridge irb** global configuration command from the configuration.
- CSCdp66822

If the **atm ilmi-pvc-discovery subinterface** command is configured on both the ATM 0/0/0 interface and an ATM subinterface, the ATM PVC will not come up after the NRP reloads, unless you do a **shut** command followed by a **no shut** command on the ATM 0/0/0 interface.

Workaround: Avoid using the **atm ilmi-pvc-discovery** command on ATM subinterfaces.

- CSCdp74289

The NRP should use “big” buffers to do IP Multicast packet replication instead of using “very big” buffers when the payload size is 1500 bytes. Since the NRP has a limited number of “very big” buffers, memory allocation failure may be seen if the payload size is 1500 bytes and IP Multicast is enabled.

Workaround: Increase the number of “very big” buffers.
- CSCdp74444 and CSCdt39140

The system will exhibit higher than normal CPU utilization when a telnet connection is trying to send data into a TCP connection with a zero send window. This increased CPU utilization is mostly cosmetic, as higher priority tasks will continue to run normally, and packet switching should be unaffected. There is no workaround.
- CSCdr04534

On an NRP-1, during an ATM interface-flapping test in a configuration with 2000 PPPoA/40 L2TP tunnels and without any traffic, the 2000 tunnels will not all be re-established after issuing a **shut** command, pausing 5 minutes, and issuing a **no shut** command. The same test with a configuration of 1700 PPPoA/300 L2TP tunnels recovers fine. There is no workaround.
- CSCdr44333

A memory leak might happen when the NRP has 2000 PPPoA sessions with AAA authentication configured and has a very large volume of trace messages to display during NRP booting up.

Workaround: Turn off console logging. (The NRP should turn off console logging as a normal operation.)
- CSCdr50376

If you turn on traffic shaping on 400 or more PVCs, and heavy traffic causes the PVCs to become congested simultaneously, random PPP sessions might be dropped.

Workaround (do one of the following):

 - Turn off PPP keepalives
 - Reduce the number of traffic-shaped PVCs
- CSCdr82324

When 800 sessions are brought up through the home gateway, NRP-1, and L2TP access concentrators, the send-receive counters are out-of-sync and the tunnels are torn down. Under these circumstances, all sessions are terminated. There is no workaround.
- CSCdr88684

When SSG is enabled on the NRP, issuing the **clear interface ATM 0/0/0** command causes the NRP to reload.

This behavior is observed *only* when SSG is enabled on the NRP and does not happen when SSG has been disabled with the **no ssg enable** command.

Workaround: When SSG is enabled on the NRP, do not issue the **clear interface ATM 0/0/0** command during any ATM traffic volume.

Alternative workaround: When SSG is enabled on the NRP, after issuing a **shut** command on the ATM interface, wait at least 10 minutes before issuing a **no shut** command.
- CSCds24692

When memory corruption causes the NRP to reload, the reload-information file might not include the dump of the corrupted memory that caused the reload. There is no workaround.

- CSCds29915

With frequent CLI operations on the ATM interface (for example, reconfiguration commands, commands to clear the interface, etc.) during heavy traffic, the NRP might have a bus-error crash in the packet-receiving path.

Workaround: Avoid frequent CLI operations on the ATM interface during heavy traffic.
- CSCds44174

The **aaa accounting update** command does not change the frequency of the accounting updates that are sent to the RADIUS server. There is no workaround.
- CSCds50474

An NRP loses its Tag Distribution Protocol (TDP) or Open Shortest Path First (OSPF) neighbor relationship with the downstream router when traffic of 35K packets per second (pps) at 64byte packets is sent. Performance tests indicate that the NRP is able to sustain at least 45K pps. At 32K pps at 64 byte packets, the NRP drops about 1.78 percent of the packets but does not lose the TDP/OSPF neighbor relationship.

Using the **scheduler allocate 4000 200** command results in a slightly improved performance but the TDP/OSPF neighbor relationship is still lost, albeit at a somewhat higher traffic load. There is no workaround.
- CSCds51983

When SSG is enabled, it is possible to configure NetFlow with the **ip route-cache flow** command, assuming that the **ip cef** command was enabled previously. However, this is not supported by SSG and will short-circuit the SSG functionality.

Workaround: Use the **no ip route-cache flow** command to prevent the problem.
- CSCds57906

While reconfiguring PVCs on the NRP, you might experience an unexpected reload after a message similar to the following message:

```
19:12:03: %SYS-3-MGDTIMER: Uninitialized timer, timer stop, timer = 61406F10.
-Process= "Virtual Exec", ipl= 0, pid= 41
```

There is no workaround.
- CSCds61231

On a Cisco 6400, when an ATM interface is configured with RBE with IP unnumbered, static routes are not created if dynamic addresses are handed out using a Cisco IOS DHCP server. The addresses are handed out correctly by the Cisco IOS DHCP server, but the static routes are not built in the routing table.

Workaround: Use an external DHCP server.
- CSCds79395

Under rare circumstances, and more likely when IP NAT is used, an NRP might reload with the following message:

```
%SYS-3-BADMAGIC: Corrupt block at 624D0C38 (magic 0D0D0D0D)
```

This error might be caused by process writing beyond the allocated memory. There is no workaround.
- CSCdt01465

On an NRP running Cisco IOS Release 12.1(3)DC1 or subsequent releases, MS NetMeeting might not function correctly if NAT is employed. There is no workaround.

- CSCdt05069
In a PPPoE session between an NRP and a Cisco 7500 series router, the NRP might not be able to send a “RADIUS attribute 8 (framed-ip-address)” in its accounting “stop” packet. There is no workaround.
- CSCdt42340
Allocation of a negative number of bytes might cause a watchdog-forced reload of the NRP. There is no workaround.
- CSCdt44101
In a configuration with a fully-meshed BGP configured between provider edge (PE) routers, and with MPLS enabled on all PE routers, a Cisco 6400 connected to an ATM-LSR core reloads unexpectedly after the LSC reboots several times.
Workaround: Disable MPLS on the PE routers.
- CSCdt45145
Upon a failover of a redundant NSP, some PVCs on the NRP might stop transmitting cells over the ATM interface.
Workaround: Issue a **shut** command followed by a **no shut** command on the subinterface (not on the main interface).
Alternative workaround: Remove and reapply the PVCs (using CLI commands) and reboot the NRP.
- CSCdt47374
Resetting a virtual interface while SNMP polls for interface information might cause a bus-error exception. There is no workaround.
- CSCdt47730
In a configuration that uses the NSP as a Label Switch Router (LSR) and the NRP as a Label Edge Router (LER), if the NSP is reloaded while the NRP is up, two problems might be observed:
 - a. The NRP loses the Open Shortest Path First (OSPF)-neighbor relationship with the NSP
 - b. The XtagATM interfaces are down
 Both symptoms disappear if the NRP is reloaded subsequently. Occasionally, the NSP reload causes an unexpected reload of the NRP.
Workaround: Reload the NRPs after a NSP reload.
- CSCdt53551 and CSCdt68843
CEF is not working properly for an ATM-to-ATM path. When a PPPoA user is logged in to a SSG pass-through service and CEF is enabled globally, both upstream and downstream packets are CEF-switched. However, when CEF is enabled globally and disabled only at the uplink ATM sub-interface, both upstream and downstream packets are not CEF-switched. For an ATM-to-GE path, CEF is working fine. There is no workaround.
- CSCdt65265
In an NRP-SSG L2TP configuration, the number of sessions that an NRP can handle diminishes under extremely heavy traffic. There is no workaround.
- CSCdt65698
An NSP switchover might cause an NRP installed in slots 5, 6, 7, and/or 8 to reset.
Workaround: do not install NRPs in slots 5 through 8 but use other slots.

- CSCdt67753
On a Cisco 6400 running Cisco IOS Release 12.1(4)DC or subsequent releases and acting as an L2TP Network Server, the default Maximum Transmission Unit (MTU) on the virtual-access interfaces is 1460. If the end host attempts to use the maximum MTU and TCP Path MTU Discovery is not working because some routers block Internet Control Message Protocol (ICMP) messages, this might cause connectivity to break for certain clients.
Workaround: Configure **ip mtu 1501** on the virtual-template interface.
- CSCdt73695
The HTTP Redirect feature is not supported for subscribers connecting to SSG using RBE. There is no workaround.
- CSCdt74755 and CSCdp05523
Using NAT on an NRP causes high CPU utilization. There is no workaround.
- CSCdt75956
If only a few users download a large file in an NRP-SSG PPPoE configuration, the utilization of the NRP CPU might grow to more than 10 percent. There is no workaround.
- CSCdt76953
When multiple PPPoE clients log on/log off to/from NRP-SSG L2TP services, the amount of memory held by the “Net Background” increases proportionally with the number of sessions that log on/log off. There is no workaround for this memory leak.
- CSCdt77367
If SSG cannot perform CEF because a route to the next hop is not available, SSG does not jump to the next switching path (that is, to Fast Switching). There is no workaround.
- CSCdt77978
When clients destroy a PPPoE session ungracefully, the process PPP manager might hold a small amount of memory and does not return it to the processor. There is no workaround.

Caveats that Apply to the NRP-1 Only

- CSCdt46059
An NRP-1 running Cisco IOS Release 12.1(4)DC1 or subsequent releases might reload unexpectedly with a bus error for an unknown reason. The address combined with the return of the **show region** command indicate a software crash by accessing a non-existent address. There is no workaround.
- CSCdt69743 and CSCdt69881
A slow memory leak might occur on an NRP-1, which is related to PPPOE authentication. With the configuration of 128 MB RAM and an average of 200 to 300 concurrent users (VPDN sessions), the memory of the NRP is exhausted after three to four weeks and the NRP needs to be reloaded.
Workaround: Reload the NRP-1 approximately every two weeks.

Caveats that Apply to the NRP-2 Only

The following open caveats apply only to the NRP-2.

- CSCdr55905

The NRP-2 configuration is held on the NSP PCMCIA Disk. When you attempt to save the configuration on the NRP-2, the process on the NSP currently does not check for available disk space before trying to write the configuration to the disk. This might cause the file to be stored on the disk incompletely, or not at all. Generally this is not an issue, because a chassis alarm is generated when the disk space gets low.

Workaround: Check the disk space on the NSP and check any disk alarms before saving NRP-2 configurations.

- CSCdr70852

The compress-configuration option is not currently available for the NRP-2 platform. The configuration command **service compress-config** is currently ignored and configurations are saved uncompressed. There is no workaround.

- CSCdr76980

The NSP disk-format operations to the PCMCIA disk in slot 1 might affect concurrent disk operations to the disk in slot 0.

Workaround: As the disk in slot 0 is used for storing NRP-2 system configuration, the user should not perform formatting operations on disk 1 while the NRP-2 uses disk 0.

- CSCdr83804

The NRP-2 booting and configuration operations depend on the presence of the PCMCIA disk in slot 0 of the NSP. Removal of that disk during NRP-2 disk operations, including booting and the saving of configurations, may result in an unexpected reload of the NRP-2.

Workaround: Assure that no NRP-2 disk operations are in progress before removing the PCMCIA disk from slot 0 of the NSP.

- CSCdr88742

The NRP-2 running configuration is saved on the NSP PCMCIA disk. If that disk is not present, the configuration cannot be saved. The current NRP-2 software does not warn the user if the configuration has not been saved correctly.

Workaround: Make sure that the PCMCIA disk is present on the NSP before saving the NRP-2 running configuration.

- CSCdr95295

The total memory size displayed for the NRP-2 in response to the **show version** command is incorrect. Systems with 512 MB installed display the following memory size:


```
cisco NRP2SP (NRP2SP) processor with 393216K/196608K bytes of memory.
```

The second value, the installed I/O memory, is too large by 64MB. Systems with 256 MB installed also show an I/O memory value that is too large by 64MB. There is no workaround.

- CSCdr98773

When an ATM subinterface is configured, it does not show up in the running configuration.

Workaround: Issue the **show ip interface** command or the **show interface** command to show the ATM subinterface.

- CSCds02020
 Resetting the NRP-2 with the **hw-module slot x reset** NSP command while the NRP-2 has pending console output, causes bus error warning messages to appear on the NSP console and in the NSP error log. Although there is no workaround, the messages are simply a warning and are harmless.
- CSCds26319
 When an NRP-2 receives traffic that exceeds the Maximum Transmission Unit (MTU) specified on that NRP-2, the virtual access (VA) interfaces counter displays incorrect values. After issuing the **show controller** <atm0/0/0> command, the counter for giant packets (rx_drop_giant) displays the incorrect values.
 Workaround: Use the giant discard statistic counter (rx_giant_discard) in the **show controller** <atm0/0/0> command to adjust the number shown in the giant packets counter in the following manner:
 total giants discarded = (rx_drop_giant) minus (rx_giant_discard/2)
- 

Note Both rx_drop_giant and rx_giant_discard are cumulative counters.

- CSCds47327
 When a PPPoE session (on an ATM subinterface) is up and the ATM subinterface is shut on the NRP-2 LAC, the following message is logged on the NRP-2 console:

```
1d03h: %NRP2_SE64-3-ULD_BADVC: ATM0/0/0 bad vcd 2002 packet - 07D28000 AAAA0300 80C20007 000000D0
BA706B2B 00D0BA70
```

 This message is due to a timing-race condition in shutting down PVCs within the SAR driver. There is no workaround.
- CSCds66638
 When a PPPoE session is up, the NRP-2 drops sweep ping packets with a size is greater than 4000 bytes. There is no workaround.
- CSCds83542
 While bringing up 4000 L2TP sessions on an LNS, spurious memory reads might be generated and might cause an “ALIGN-3-SPURIOUS” error message. Although there are no known negative effects of this problem, there is no workaround.
- CSCds83689
 Some sessions do not come up when the ATM interface of either the LAC or the LNS is flapped many times. The test configuration has 4000 PPPoA sessions and uses a ppp-keepalive interval value of 10.
 Workaround: Increase the keepalive interval to 200 (as per the recommended scalability guidelines).
- CSCdt15119
 Intermediate System-to-Intermediate System (IS-IS) routing updates are not sent with “AAL5NLPID” encapsulation. IS-IS/Connectionless Network Service (CLNS) updates from other routers are not seen by the NRP-2, but the NRP-2 sends out the routing updates of it's own networks. There is no workaround.
- CSCdt19637 and CSCds79849
 An NRP-2 configured with a large number of PPP sessions may report a “%SYS-3-CPUHOG” error message when the **clear counters** command is issued at the router's prompt. There is no workaround.

- CSCdt37234

The NRP-2 stops passing traffic on interface “ATM0/0/0” in Cisco IOS Release 12.1(4)DC1 or subsequent releases. Issuing the **shut** command followed by the **no shut** command on the “ATM0/0/0” interface temporarily solves the problem. Debugging the ATM error on the NRP-2 shows the following error message (date and time will differ):

```
Feb 5 14:38:05: ATM(ATM0/0/0.5003): VC(1418) Bad SAP received
```

There is no workaround.

- CSCdt46733

In a configuration with auto negotiation enabled and using the Cisco 7505 router as Pageant generator, sending constant traffic through the GE interface to the NRP-2 at a speed of nearly 40 Kpps and with a packet size of about 1024 bytes, will cause the NRP-2 to stop receiving traffic from the Cisco 7505 router after about 10 minutes. The interface will recover after issuing a **clear interface** command or a **shut** command followed by a **no shut** command.

Workaround: Do not configure auto negotiation for the GE interface in the above-mentioned configuration.

- CSCdt51547

With many ATM subinterfaces configured on a Cisco 6400, the **ip verify unicast reverse-path** command might incorrectly drop a fraction of incoming traffic. There is no workaround.

- CSCdt51810

An unexpected reload might occur when a Cisco 6400 loses its Tag Distribution Protocol (TDP)-neighbor relationship with a neighboring router due to extremely high data loads. This unexpected reload has only occurred in lab testing when injecting a steady data stream that overruns the router's ability to process the data.

Workaround: Use the **tag-switching tdp discovery hello hold <time>** command to increase the TDP timeout on both routers so that TDP-neighbor loss is less likely to occur. To check the current parameters, use the **show tag-switching tdp parameters** command.

- CSCdt65960

A Cisco 6400 running Cisco IOS Release 12.1(4)DC1 or subsequent releases is not able to prevent Telnet access to routers using an access list (ACL), because the access-class command which is used to tie the ACL to the virtual terminal (VTY) interfaces is ignored. There is no workaround.

- CSCdt74760

After the configuration of range-PVC entries together with PVC entries on one subinterface, the configuration of the range-PVC entries is lost during a reboot of the NRP-2. There is no workaround.

Resolved Caveats—Release 12.1(5)DC

This section describes caveats that have been closed and resolved in Cisco IOS Release 12.1(5)DC. Caveats that were already closed and resolved in previous releases are not included in this section.

Caveats that Apply to Both the NRP-1 and NRP-2

- CSCdp38668, CSCdp52852, and CSCdr63668

After a long period of correct operation and with the Network Access Server port ID format “d” enabled, RADIUS authentication requests and accounting records associated with certain PVCs begin to carry incorrect information (mostly zeros).

Workaround: Remove the problem PVCs and recreate them on the NRP.

This caveat was already resolved in Cisco IOS Release 12.1(4)DC.

- CSCdr54230

A Border Gateway Protocol (BGP) UPDATE contains Network Layer Reachability Information (NLRI) and attributes that describe the path to the destination. Each path attribute is a type, length, value (TLV) object.

The type is a two-octet field that includes the attribute flags and the type code. The fourth high-order bit (bit 3) of the attribute flags is the Extended Length bit. It defines whether the attribute length is one octet (if set to 0) or two octets (if set to 1). The extended length bit is used only if the length of the attribute value is greater than 255 octets.

The AS_PATH (type code 2) is represented by a series of TLVs (or path segments). The path segment type indicates whether the content is an AS_SET or AS_SEQUENCE. The path segment length indicates the number of autonomous systems (ASes) in the segment. The path segment value contains the list of ASes (each AS is represented by two octets).

The total length of the attribute depends on the number of path segments and the number of ASes in them. For example, if the AS_PATH contains only an AS_SEQUENCE, then the maximum number of ASes (without having to use the extended length bit) is 126 [= (255-2)/2]. If the UPDATE is propagated across an AS boundary, then the local Abstract Syntax Notation (ASN) must be appended and the extended length bit used.

The caveat was caused by the mishandling of the operation during which the length of the attribute was truncated to only one octet. Because of the internal operation of the code, the receiving border router would not be affected, but its iBGP peers would detect the mismatch and issue a NOTIFICATION message (update malformed) to reset their session.

The average maximum AS_PATH length in the Internet is between 15 and 20 ASes, so there is no need to use the extended length. The failure was discovered because of a malfunction in the BGP implementation of another vendor. There is no workaround.

This caveat was already resolved in Cisco IOS Release 12.1(4)DC1.

- CSCdr56802

Traffic shaping configuration using the **vbr-nrt** *<pcr> <scr> <input burst>* under VC-class command cannot be removed by entering **no vbr-nrt** *<pcr> <scr> <input burst>*.

Workaround: Remove the entire VC-class, and re-enter the VC-class configuration without traffic shaping

This caveat is resolved in Cisco IOS Release 12.1(5)DC..

- CSCds04747

Cisco IOS software contains a flaw that permits the successful prediction of TCP Initial Sequence Numbers.

This vulnerability is present in all released versions of Cisco IOS software running on Cisco routers and switches. It only affects the security of TCP connections that originate or terminate on the affected Cisco device itself; it does not apply to TCP traffic forwarded through the affected device in transit between two other hosts.

To remove the vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is described in DOTS record CSCds04747.

Workarounds are available that limit or deny successful exploitation of the vulnerability by filtering traffic containing forged IP source addresses at the perimeter of a network or directly on individual devices.

This notice will be posted at <http://www.cisco.com/warp/public/707/ios-tcp-isn-random-pub.shtml>.

This caveat was already resolved in Cisco IOS Release 12.1(4)DC2.

- CSCds10123

The PPP authentication process might cause a memory leak. This is most likely to happen when the 6400 is terminating a large number of PPP sessions and there is a high level of PPP-authentication processing. There is no workaround.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.

- CSCdt14663

In a configuration with CEF enabled and virtual access precloned, about 15% of the packets might be lost during the first minute of a PPPoE session. After one minute the problem disappears and everything works fine.

Workaround: Disable CEF and disable precloning.

This caveat was already resolved in Cisco IOS Release 12.1(4)DC1.

- CSCds21838, CSCdt33723, and CSCdt42161

When a PPP client or SSD (when a user tries to log in to SSG using PPP or the web) sends an authentication request to SSG, SSG will treat the authentication request as a proxy and forwards it to a RADIUS server. If there is no reply from the RADIUS server, SSG will not resend the request to the RADIUS server. There is no workaround.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.

- CSCds25422

When using IP multicast, the NRP might report “CPUHOG” errors, referencing the PIM and IGMP processes. These errors indicate that the processes are not relinquishing the CPU often enough to allow other packet-handling processes to perform. In extreme cases, this can lead to severe degradation in performance. There is no workaround.

This caveat is closed in Cisco IOS Release 12.1(5)DC.

- CSCds29890

When using multiple RADIUS servers, failure or lack of performance of one of the servers can prevent SSG from using one of the other servers. There is no workaround.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.

- CSCds32217 and CSCdr61016

Multiple Cisco IOS software and CatOS software releases contain several independent but related vulnerabilities involving the unexpected creation and exposure of SNMP community strings. These vulnerabilities can be exploited to permit the unauthorized viewing or modification of affected devices.

To remove the vulnerabilities, Cisco is offering free software upgrades for all affected platforms. The defects are documented in DDTs records CSCds32217, CSCds16384, CSCds19674, CSCdr59314, CSCdr61016, and CSCds49183.

In addition to specific workarounds for each vulnerability, affected systems can be protected by preventing SNMP access.

This notice will be posted at

<http://www.cisco.com/warp/public/707/ios-snmp-community-vulns-pub.shtml>.

CSCdr61016 was already resolved in Cisco IOS Release 12.1(4)DC and CSCds32217 was already resolved in Cisco IOS Release 12.1(4)DC2.

- CSCds53978 and CSCds28026

During configuration, the NRP might unexpectedly reload with the following error message:

```
%ALIGN-1-FATAL: Corrupted program counter
```

This behavior might be due to a race condition in which a function might be called before its initialization. There is no workaround.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.

- CSCds40538 and CSCds43050

A configuration with PPPoA/SSG and NetMeeting may cause a red-zone violation and a reload on the NRP. There is no workaround.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.

- CSCds54182

An NRP that is running Cisco IOS Release 12.1(1)DC1 and that has 1900+ access interfaces and memory compression configured, experiences memory fragmentation: the largest block is about 45 KB and the free memory is 20 MB.

Workaround: Configure a free list size for the compression history block, using the **memory free-list number** command.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.

- CSCds57575

When the NRP is reloaded with a dead switch port, the NRP attempts to bring up the FE interface. The NRP reports the interface status as “reset with line down” instead of reporting the interface as down. There is no workaround.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.

- CSCds61975 and CSCdr29259

The packets-out counter on the Virtual-Access interface of a Cisco 6400 LNS might be incorrect when the L2TP tunnel and the outgoing traffic use the same physical interface and CEF is enabled.

Workaround: Disable CEF.

This caveat was already resolved in Cisco IOS Release 12.1(4)DC.

- CSCds65995

When using “dot1q” encapsulation on the Cisco 6400 and the native VLAN is VLAN 1, the communication between the devices stops.

Workaround: Use ISL instead of “dot1q” encapsulation.

Alternate workaround: Change the native VLAN to a VLAN other than VLAN 1.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.
- CSCds75540

If an ambiguous command (for example, **config-if-atm-ran**) is entered while in the PVC range configuration submode, a spurious memory traceback message will be displayed when the next command is entered. The traceback message is harmless.

Workaround: Do not enter incomplete commands while in the PVC range configuration submode.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.
- CSCds76299 and CSCds43050

The NRP might reload with the following error message:

```
%SYS-3-OVERRUN: Block overrun at 627E418 (red zone = 4E205047)
```

This error is caused by process writing beyond the allocated memory. There is no workaround.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.
- CSCds76530 and CSCds43050

An NRP running Cisco IOS Release 12.1(3)DC1 or subsequent releases might reload due to malloc failures and might produce error messages such as the following ones:

```
%SYS-2-MALLOCFAIL: Memory allocation of 788 bytes failed from 0x6025A258, pool I/O, alignment 32 -Process= "Syslog Traps", ipl= 7, pid= 75
```

or

```
%SYS-2-MALLOCFAIL: Memory allocation of 276 bytes failed from 0x6025A258, pool I/O, alignment 32 -Process= "Net Background", ipl= 7, pid= 17
```

This is due to a memory leak which ultimately results in exhaustion of the memory resource. As a result, some process(es) fail to acquire the needed memory and the system restarts. There is no workaround.

This caveat was already resolved in Cisco IOS Release 12.1(4)DC1.
- CSCds79415 and CSCds07326

An NRP running Cisco IOS Release 12.1(3)DC might reload unexpectedly due to a bus error related to an Inverse ARP problem. There is no workaround.

This caveat was already resolved in Cisco IOS Release 12.1(4)DC.
- CSCds81465 and CSCds82868

An NRP might reload due to memory-allocation failures in the process and I/O memory. After malloc failures, the NRP eventually reloads, sometimes with redzone-violation errors and other times due to the watchdog timeout. There is no workaround.

This caveat was already resolved in Cisco IOS Release 12.1(4)DC.
- CSCds81569

After using the Belle application to modify the unspecified bit rate plus (UBR+) on VCs for a period of time, some VCs might pause indefinitely.

Workaround: issue the **clear int a0/0/0** command.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.

- CSCds83122 and CSCdr61713

After an NRP running Cisco IOS Release 12.1(3)DC or Release 12.1(3)DC1 has reloaded unexpectedly, the boot date and time stamp and the uptime might not show correctly in the output of the **show version** command.

Workaround: Restart the NRP manually.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.

- CSCds86754 and CSCds69248

With NAT and Policy Based Routing (PBR) configured together on the NRP, fast switching does not work. There is no workaround.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.

- CSCds90991

When logging on and logging off consecutively with a different user name from the same host, SSG will reload. There is no workaround.

This caveat was already resolved in Cisco IOS Release 12.1(4)DC2.

- CSCds91430

The AAA authentication process on an NRP that is running Cisco IOS Release 12.1(1)DC1 or subsequent releases with a PPPoA user, experiences a long delay: After the NRP receives the Challenge Handshake Authentication Protocol (CHAP) “response” message, it takes about one minute before the CHAP answers with a “success” message, while only link control protocol (LCP) keepalives are active during the process. There is no workaround.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.

- CSCdt08279

In a PPP ATM configuration, when a remote ATM connection goes down for a period that exceeds the PPP idle-timeout value that was supplied by the AAA feature of the RADIUS server, a bus error might occur.

Workaround: Increase the PPP idle-timeout value in the AAA feature or— if possible— minimize the time that the remote ATM connection is down.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.

- CSCdt25069 and CSCds43050

An NRP might reload due to a software-forced crash related to Service Selection Gateway issues. There is no workaround.

This caveat was already resolved in Cisco IOS Release 12.1(4)DC1.

- CSCdt39828

The “vpn_select_tas” registry and related code is missing in Cisco IOS Release 12.1(3)DC1 and subsequent releases. There is no workaround.

This caveat was already resolved in Cisco IOS Release 12.1(4)DC2.

- CSCdt42145

SSG will check the RADIUS attribute length before accepting a RADIUS packet to ensure that a corrupted RADIUS packet will not affect the system.

This improvement is integrated in Cisco IOS Release 12.1(5)DC.

- CSCdt49063, CSCds24352, and CSCdt71168
An NRP might reload unexpectedly when PPPoE is used. There is no workaround.
This caveat is resolved in Cisco IOS Release 12.1(5)DC.
- CSCdt49217
RADIUS format "d" no longer works. There is no workaround.
This caveat is resolved in Cisco IOS Release 12.1(5)DC.
- CSCdt65431
The system generates a bus error when a user constantly logs on to or logs off from the PPP sessions. The problem is more likely to happen with a Windows 95 client machine. There is no workaround.
This caveat is resolved in Cisco IOS Release 12.1(5)DC.
- CSCuk21410
In a configuration that includes CEF and precloning of the virtual access, when making an initial PPPoE connection to the Cisco 6400, a packet loss of about 15 percent might occur. After one minute, the problem disappears and everything works fine.
Workaround: Disable CEF to relieve the CPU load and disable the precloning.
This caveat was already resolved in Cisco IOS Release 12.1(4)DC1.

Caveats that Apply to the NRP-1 Only

- CSCdt34231
On an NRP-1, when adding or removing subinterfaces to or from the Fast Ethernet interface, the interface may go into a down or reset state. There is no workaround.
This caveat is resolved in Cisco IOS Release 12.1(5)DC.

Caveats that Apply to the NRP-2 Only

- CSCds06375
When issuing a **shutdown** CLI command on an ATM interface with a large number (more than 1000) of VCs configured, the following "CPUHOG" message appears on the console output:
00:06:39: %SYS-3-CPUHOG: Task ran for 2744 msec (0/0), process = Exec, PC = 602A7F88.
Although the operation is unlikely to be affected by this caveat, there is no workaround.
This caveat is closed in Cisco IOS Release 12.1(5)DC because it is caused by unusual conditions that will likely only exist under development tests.
- CSCds19683, CSCds19686, and CSCds19690
Booting up an NRP-2 with a configuration that contains a large number of subinterfaces might cause the following (or very similar) "CPUHOG" message to appear on the console output:
00:07:51: %SYS-3-CPUHOG: Task ran for 49272 msec (0/0), process = Auto Config insertion process, PC = 602AFF20.
Although the operation is unlikely to be affected by this caveat, there is no workaround.
This caveat was already resolved in Cisco IOS Release 12.1(4)DC.

- CSCds70874

When an NRP-2 receives traffic that exceeds the Maximum Transmission Unit (MTU) specified on that NRP-2, the virtual access (VA) interfaces counter displays incorrect values. After issuing the **show controller** <atm0/0/0> command, the counter for giant packets (rx_drop_giant) displays the incorrect values.

Workaround: Use the giant discard statistic counter (rx_giant_discard) in the **show controller** <atm0/0/0> command to adjust the number shown in the giant packets counter in the following manner:

total giants discarded = (rx_drop_giant) minus (rx_giant_discard/2)



Note Both rx_drop_giant and rx_giant_discard are cumulative counters.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.

- CSCds61887

When a **write mem** command is issued on the NRP-2, the configuration data is sent to the NSP for storage on the NSP disk. If this disk operation fails, the NSP will issue an error message; however, the NRP-2 itself will not indicate the failure on the console.

To ensure that the configuration data has been written to the NSP disk, the user can look at the time and date stamp for the configuration file on the NSP disk. Configuration data is stored in “disk0:/slotn/NRP2-startup-config”, where “n” (in slotn) is the slot number of the NRP-2. A quick scan for error messages on the NSP console will also reveal any problems that might have occurred while writing the configuration to the NSP disk.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.

- CSCds82038

The contents of the current crashinfo file are not displayed as part of the output from the **show stacks**.

Workaround: View the current crashinfo file by using the **more nsp_slot:nrp-crashinfo-data** command of the NRP-2. The NRP-2 crashinfo files may also be viewed by looking in the appropriate slot directory on “disk0:” of the NSP.

This caveat is resolved in Cisco IOS Release 12.1(5)DC.

Preexisting NRP-1 Hardware Caveats

This section describes possible unexpected behavior by earlier hardware versions of the NRP-1. To determine your NRP-1 part number (P/N), see the section [“Determining Your NRP-1 Part Number” section on page 46](#).

- CSCdk47837—NRP-1s reset when you reload or reset a nonredundant NSP in Slot 0A.

Affected Part Numbers: 800-03785-03, 800-03655-02 or higher part numbers

Symptom:

While the NSP is in Slot 0A of a single NSP system, the NRP-1s reset during NSP reloads or resets.

Workaround:

In a nonredundant system using an NSP of P/N 800-03785-03, place the NSP in Slot 0B.

- CSCdk88262—NRP-1 ignores **boot system** command entries in the startup configuration.

Affected Part Numbers:

800-03655-01, 800-03655-02, 800-03655-03, 800-03655-04

Symptoms:

Regardless of any **boot system** global configuration command entries in the startup configuration, the NRP-1 boots the first image in Flash memory after a reset. This problem occurs after one of the following actions:

- NRP-1 power cycle
- Two or more successive resets by using the **hw-module EXEC** command on the NSP.

Workaround:

To avoid this problem, make sure that the desired image is the first file on the Flash memory device. Complete the following steps in EXEC mode:

- Enter **delete flash:*** to mark all files on the Flash memory device for deletion.
- Enter **squeeze flash:** to permanently erase all files marked for deletion.
- Use the **copy flash:** EXEC command to copy the desired image to the Flash memory device.
- Use the **dir flash:** EXEC command to verify that the image file is the first file on the Flash memory device.

Recovery:

If you encounter the problem before implementing the workaround, reset the NRP-1 once by using the **hw-module slot number reset** EXEC command on the NSP. As long as the NSP sends a single reset to the NRP-1, the NRP-1 does not ignore the **boot system** global configuration command entries in the startup configuration.

- CSCdp57387—Hot-inserting an NRP-1 might reset the adjacent NRP-1.

Affected Part Numbers:

800-03655-04, 800-03655-05, 800-03655-06

Symptoms:

With or without redundancy configured, an NRP-1 inserted into a live system might reset the NRP-1 in the adjacent slot of the slot pair. NRP-1 slot pairs are slots 1-2, 3-4, 5-6, and 7-8.

Workaround (use one of the following):

- If you are not using NRP-1 redundancy and your system contains four or fewer NRP-1s, place only one NRP-1 in each slot pair.
- If this workaround is not feasible, replace your NRP-1(s) with P/N 800-03655-07 or higher.

- CSCdr08888—NRP-1 Console port does not respond.

Affected Part Number: 800-03655-01

Symptoms:

When the terminal server is configured such that hardware flow control is enabled on the port attached to the NRP-1 console, the NRP-1 console port does not respond.

Workaround:

Configure your terminal server to disable hardware flow control on the port attached to the NRP-1 console.

- CSCdr16154—NRP-1 unrecognized card type.

Affected Part Numbers:

800-03655-01, 800-03655-02, 800-03655-03, 800-03655-04, 800-03655-05, 800-03655-06, 800-03655-07, 800-03655-08

Symptom:

NSP reports unknown cardtype when the chassis is populated primarily with NRP-1s.

Workaround (use one of the following):

- Reduce the number of NRP-1s in the system
- Make sure all the NRP-1s are P/N 800-03655-09 or higher
- Make sure the NSP is P/N 800-03785-08 or higher.

- CSCdr61340

The NRP-1 crashes during reload when both of the following conditions are met:

- NRP-1-SSG is enabled and RFC 1483 IP Routed are used together with 1750 or more sessions.
- ROMMON variable IOMEM is set to larger than 16 MB (By default, IOMEM = 36 MB)

Workaround (use one of the following):

- Disable SSG.
- Enable SSG but set the ROMMON variable IOMEM to 16 MB. Do not turn on traffic shaping.

- CSCdr82841

When the SSG is enabled after an upgrade from Cisco IOS Release 12.0(3)DC or Release 12.0(5)DC to Release 12.0(7)DC or higher, the SSG transparent passthrough feature is no longer supported.

Workaround: To enable non-SSG connections to pass through the NRP-1, disable the SSG with the **no ssg enable** command.

- CSCdr97361

The execution of the **Show ip nat translation verbose** may cause the 6400 NRP-1 to reload.

Workaround: Set the terminal length to “term len 0” before executing the **Show ip nat translation verbose**.

Determining Your NRP-1 Part Number

To determine the NRP-1 part number, use one of the following methods with the information in [Table 11](#):

- If you are holding the board, look at the 800- part number label on the back of the NRP-1.
- If you can only view the faceplate of the NRP-1, look at the CLEI code label.

- Enter the **show nrp** privileged EXEC command to display the 73- part number.

The following example displays the **show nrp** command output for an NRP-1 with part number 73-3082-06:

```
6400-nrp# show nrp
Router installed in slot 5
Network IO Interrupt Throttling:
throttle count=0, timer count=0
active=0, configured=0
netint usec=4000, netint mask usec=200
NRP CPU ID EEPROM:
Hardware revision 4.255 Board revision A0
→ Serial number 12346818 Part number 73-3082-06
Test history 0x0 RMA number 00-00-00
EEPROM format version 2
EEPROM contents (hex):
0x00: 02 E3 04 FF 00 BC 65 C2 49 0E 26 05 00 00 00 00
0x10: 50 00 00 00 07 CF 04 09 00 00 00 78 00 00 00 00
6400-nrp#
```

Table 11 NRP-1 Part Numbers

CLEI Code	800- Part Number	73- Part Number
BAC5EEPDA A	800-03655-01	73-3082-03
BAC5EEPDA B	800-03655-02	73-3082-04
BAC5EEPDA C	800-03655-03	73-3082-05
BAC5EEPDA D	800-03655-04	73-3082-06
BAC5EEPDA E	800-03655-05	73-3082-07
BAC5EEPDA F	800-03655-06	73-3082-08
BAC7RUBCA A	800-03655-07	73-3082-09
BAC7RUBCA B	800-03655-08	73-3082-10
BAC7VUBCA A	800-03655-09	73-3082-11

Related Documentation

The following sections describe the documentation available for the Cisco 6400 universal access concentrator. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com and the Documentation CD-ROM.

Use these release notes with these documents:

- [Release-Specific Documents, page 48](#)
- [Platform-Specific Documents, page 48](#)
- [Feature Modules, page 50](#)
- [Cisco IOS Software Documentation Set, page 50](#)

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.1 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes*

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Release Notes

On the Documentation CD-ROM at:

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

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

Technical Documents

- *Caveats for Cisco IOS Release 12.1* and *Caveats for Cisco IOS Release 12.1 T*

As a supplement to the caveats listed in the “[Software Caveats](#)” section in these release notes, see *Caveats for Cisco IOS Release 12.1* and *Caveats for Cisco IOS Release 12.1 T*, which contain caveats applicable to all platforms for all maintenance releases of Release 12.1.

On Cisco.com:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Release Notes: Caveats

On the Documentation CD-ROM:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Caveats



Note

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

Platform-Specific Documents

The documents listed in [Table 12](#) are available for the Cisco 6400 UAC on Cisco.com and the Documentation CD-ROM.

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

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

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

Aggregation Solutions: Cisco 6400 Universal Access Concentrator

Table 12 Platform Documents for the Cisco 6400 Universal Access Concentrator

Document Title	Chapter Topics
<i>Cisco 6400 UAC Hardware Installation Guide</i>	<ul style="list-style-type: none"> About This Manual Hardware Description Preparing for Installation Installing the Cisco 6400 Troubleshooting Maintaining the Cisco 6400 System Specifications Glossary Configuration Worksheets Installing the AC-Input Power Shelf and Power Supply
<i>Cisco 6400 UAC Site Planning Guide</i>	<ul style="list-style-type: none"> About This Guide Cisco 6400 Overview Site Planning Considerations System Specifications Cabling Specifications Glossary
<i>Regulatory Compliance and Safety Information for the Cisco 6400</i>	<ul style="list-style-type: none"> Overview of the Cisco 6400 Universal Access Concentrator General Documentation Information Agency Approvals Translated Safety Warnings Cisco.com
<i>Cisco 6400 UAC Software Configuration Guide and Command Reference</i>	<ul style="list-style-type: none"> About This Guide Product Overview and Configuration Cisco IOS Software Fundamentals Using the Web Console Configuring the NSP Configuring System Features Configuring the NRP Configuring Interfaces Command Reference MIB Information Resolving Error Messages Glossary
<i>Cisco 6400 FRU Installation and Replacement</i>	<ul style="list-style-type: none"> Tools and Equipment Required General Safety Precautions and Maintenance Guidelines Replacing the Front Cover Powering Down the System Backing Up the PCMCIA Card Maintaining the Air Filter Replacing an NSP Module Replacing an NRP Module Installing or Replacing a Half-Height NLC Replacing a PEM Replacing the Blower Module and Fans Verifying Plug-In Module and Component Installation

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.1 DC and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1: New Feature Documentation: New Features in 12.1-Based Limited Lifetime Releases: New Features in Release 12.1 DC

On the Documentation CD-ROM at:

Cisco IOS Software Configuration: Cisco IOS Release 12.1: New Feature Documentation: New Features in 12.1-Based Limited Lifetime Releases: New Features in Release 12.1 DC

Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

Cisco Feature Navigator is available 24 hours a day, 7 days a week. To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions at <http://www.cisco.com/register>.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM, unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On Cisco.com and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1: Configuration Guides and Command References

On the Documentation CD-ROM at:

Cisco IOS Software Configuration: Cisco IOS Release 12.1: Configuration Guides and Command References

Cisco IOS Release 12.1 Documentation Set Contents

Table 13 lists the contents of the Cisco IOS Release 12.1 software documentation set, which is available in electronic form and in printed form, if ordered.



Note

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

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.1

On the Documentation CD-ROM at:

Cisco IOS Software Configuration: Cisco IOS Release 12.1

Table 13 Cisco IOS Release 12.1 Documentation Set

Books	Major Topics
<ul style="list-style-type: none"> <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> <i>Cisco IOS Configuration Fundamentals Command Reference</i> 	Configuration Fundamentals Overview Cisco IOS User Interfaces Cisco IOS File Management Cisco IOS System Management Cisco IOS User Interfaces Commands Cisco IOS File Management Commands Cisco IOS System Management Commands
<ul style="list-style-type: none"> <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume I</i> <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume II</i> 	Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ Serial Tunnel and Block Serial Tunnel Commands LLC2 and SDLC Commands IBM Network Media Translation Commands SNA Frame Relay Access Support Commands NCIA Client/Server Commands Airline Product Set Commands

Table 13 Cisco IOS Release 12.1 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Dial Services Configuration Guide: Terminal Services</i> • <i>Cisco IOS Dial Services Configuration Guide: Network Services</i> • <i>Cisco IOS Dial Services Command Reference</i> 	<ul style="list-style-type: none"> Preparing for Dial Access Modem Configuration and Management ISDN and Signaling Configuration PPP Configuration Dial-on-Demand Routing Configuration Dial-Backup Configuration Terminal Service Configuration Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Networks X.25 on ISDN Solutions Telco Solutions Dial-Related Addressing Services Dial Access Scenarios
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	<ul style="list-style-type: none"> Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces
<ul style="list-style-type: none"> • <i>Cisco IOS IP and IP Routing Configuration Guide</i> • <i>Cisco IOS IP and IP Routing Command Reference</i> 	<ul style="list-style-type: none"> IP Overview IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> • <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i> • <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i> 	<ul style="list-style-type: none"> AppleTalk and Novell IPX Overview Configuring AppleTalk Configuring Novell IPX
<ul style="list-style-type: none"> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i> 	<ul style="list-style-type: none"> Overview Configuring Apollo Domain Configuring Banyan VINES Configuring DECnet Configuring ISO CLNS Configuring XNS
<ul style="list-style-type: none"> • <i>Cisco IOS Multiservice Applications Configuration Guide</i> • <i>Cisco IOS Multiservice Applications Command Reference</i> 	<ul style="list-style-type: none"> Multiservice Applications Overview Voice Video Broadband
<ul style="list-style-type: none"> • <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	<ul style="list-style-type: none"> Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms Quality of Service Solutions

Table 13 Cisco IOS Release 12.1 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	Security Overview Authentication, Authorization, and Accounting (AAA) Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Configuring Passwords and Privileges Neighbor Router Authentication Configuring IP Security Options
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Cisco IOS Switching Services Overview Cisco IOS Switching Paths Cisco Express Forwarding NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
<ul style="list-style-type: none"> • <i>Cisco IOS Wide-Area Networking Configuration Guide</i> • <i>Cisco IOS Wide-Area Networking Command Reference</i> 	Introduction: Wide-Area Networking Overview Configuring ATM Configuring Frame Relay Configuring Frame Relay-ATM Interworking Configuring SMDS Configuring X.25 and LAPB
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Master Index</i> • <i>Cisco IOS Command Reference Master Index</i> • <i>Cisco IOS Debug Command Reference</i> • <i>Cisco IOS Dial Services Quick Configuration Guide</i> • <i>Cisco IOS Software System Error Messages</i> • <i>Cisco IOS Configuration Guide Master Index</i> • <i>New Features in 12.1-Based Limited Lifetime Releases</i> • <i>New Features in Release 12.1 T</i> • Release Notes (Release-note and caveat documentation for 12.1-based releases and various platforms) 	

**Note**

The *Cisco Management Information Base (MIB) User Quick Reference* publication is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco Connection Online. From Cisco.com, click on the following path: **Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB.**

Obtaining Documentation

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

World Wide Web

The most current Cisco documentation is available on the World Wide Web at <http://www.cisco.com>. Translated documentation can be accessed at http://www.cisco.com/public/countries_languages.shtml.

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

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

Documentation Feedback

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

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

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

<http://www.cisco.com>

Technical Assistance Center

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

Contacting TAC by Using the Cisco TAC Website

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

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

P3 and P4 level problems are defined as follows:

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

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

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

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

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

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

Contacting TAC by Telephone

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

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

P1 and P2 level problems are defined as follows:

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

This document is to be used in conjunction with the documents listed in the [“Related Documentation” section on page 47](#)

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

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

Copyright © 2001–2002, Cisco Systems, Inc.
All rights reserved.