



# Release Notes for Cisco 6400 NRP for Cisco IOS Release 12.1(3) DC

---

February 18, 2002

Cisco IOS Release 12.1(3) DC2

78-10959-02 Rev. E0

These release notes for the Cisco 6400 node route processor (NRP) describe the enhancements provided in Cisco IOS Release 12.1(3) DC2. These release notes are updated as needed.

For a list of the software caveats that apply to Release 12.1(3) DC2, see the “Software Caveats” section on page 12 and *Caveats for Cisco IOS Release 12.1 T*. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) 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 Connection Online (CCO) and the Documentation CD-ROM.

## Contents

These release notes describe the following topics:

- System Requirements, page 2
- New and Changed Information, page 6
- Software Caveats, page 12
- Preexisting NRP Hardware Caveats, page 18
- Related Documentation, page 21
- Obtaining Documentation, page 27
- Technical Assistance Center, page 28



---

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

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

78-10959-02 Rev. E0

# System Requirements

This section describes the system requirements for Cisco IOS Release 12.1(3) DC2:

- Memory Recommendations, page 2
- Hardware Supported, page 2
- Software Compatibility, page 2
- Determining the Software Version, page 3
- Upgrading to a New Software Release, page 3
- Feature Table, page 3

## Memory Recommendations

**Table 1** Memory Recommendations for the Cisco 6400 NRP

Product Names	Image Names	Recommended Main Memory
IOS NRP	c6400r-g4p5-mz	In most configurations, 64 MB DRAM is adequate for 750 sessions. More sessions require 128 MB DRAM. For an upgrade from an earlier release to Cisco IOS Release 12.1(1)DB1, 128 MB DRAM is recommended.
IOS NRP-MD	c6400r-boot-mz	
IOS NRP-MD W/ WEB SELECTION		

## Hardware Supported

Cisco IOS Release 12.1(3) DC2 supports the Cisco 6400 NRP. For detailed descriptions of the new hardware features, see the “New and Changed Information” section on page 6.

## Software Compatibility

Cisco recommends that Cisco IOS Release 12.1(3) DC2 be used concurrently with Cisco IOS Release 12.1(3) DB for the Cisco 6400 node switch processor (NSP). For information about Release 12.1(3) DB for the NSP, see the *Release Notes for Cisco 6400 Node Switch Processor (NSP) for Cisco IOS Release 12.1(3) DB*.

For NRP-Service Selection Gateway (SSG) users, Cisco IOS Release 12.1(3) DC2 works with the Cisco Service Selection Dashboard (SSD) version 2.2. To use the Single-Host Logon feature, you can install and configure Cisco SSD version 2.2S(1.12). However, note that both Cisco SSD version 2.2 and version 2.2S(1.12) have not completed a full-production release cycle and therefore are considered nonsupported software versions. Cisco SSD version 2.5(1) will be a fully supported production-release version that will also support Single-Host Logon, and is scheduled to be available in November 2000.

## 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(3) 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](http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/softnote/upgradsw.htm)

For general information about upgrading to a new software release, see the product bulletin *Cisco IOS Upgrade Ordering Instructions* located at:

[http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957\\_pp.htm](http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm)

If you do not have an account on CCO 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 CCO 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 Table

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 image called c6400r-g4p5-mz in this release.



### Note

Table 2 contains a selected list of features. The table is not a cumulative or complete list of all the features in this image.

**Table 2 Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.1(3) DC2**

<b>Layer 2 and Layer 3 Protocols</b>	Address Resolution Protocol (ARP)
	Internet Protocol Control Protocol (IPCP)
	Internet Protocol (IP) forwarding
	IP host
	IP multicast
	Integrated routing and bridging (IRB)
	Layer 2 Tunnel Protocol (L2TP)
	Multilink Point-to-Point Protocol (MLPPP or MLP)
	Multiprotocol Label Switching (MPLS)
	Point-to-Point Protocol (PPP) over Asynchronous Transfer Mode (ATM)
	PPP over Ethernet
	Route bridge encapsulation (RBE)
	Routed RFC1483 encapsulation
	Transmission Control Protocol (TCP)
	Telnet
	Trivial File Transfer Protocol (TFTP)
	User Datagram Protocol (UDP)
Transparent bridging	
Virtual LAN (VLAN)	
<b>Layer 3 Routing Protocols</b>	Border Gateway Protocol version 4 (BGP4)
	Enhanced Interior Gateway Routing Protocol (EIGRP)
	Intermediate System-to-Intermediate System (IS-IS)
	Open Shortest Path First (OSPF)
	Protocol Independent Multicast (PIM)
	Routing Information Protocol (RIP)
	Web Cache Coordination Protocol (WCCP) version 2
<b>Network Management, Security</b>	Authentication, authorization, and accounting (AAA)
	Challenge Handshake Authentication Protocol (CHAP)
	File Transfer Protocol (FTP)
	Network Address Translation (NAT)
	Password Authentication Protocol (PAP)
	Remote Dial-In User Service (RADIUS)
	Simple Network Management Protocol (SNMP)
	Terminal Access Controller Access Control System Plus (TACACS+)
<b>LAN Interfaces</b>	ATM (OC-3, OC-12, DS3)
	Ethernet (10BaseT)
	Fast Ethernet (100BaseTX)

**Table 2** *Features Supported by the Cisco 6400 NRP in Cisco IOS Release 12.1(3) DC2 (continued)*

<b>NRP Service Selection Gateway</b>	RADIUS accounting and interim accounting
	Service Selection Gateway (SSG) default network
	SSG autologon service
	SSG automatic service access order manipulation
	SSG Cisco express forwarding (CEF) support
	SSG Domain Name System (DNS) fault tolerance
	SSG DNS selection
	SSG full username RADIUS attribute
	SSG idle timeout
	SSG Cisco IOS NAT support
	SSG IPCP subnet mask
	SSG local forwarding
	SSG local profile
	SSG L2TP web selection
	SSG multicast support
	SSG proxy service
	SSG sequential and concurrent service access
	SSG service-defined cookie
	SSG service profile order selection
	SSG session timeout
	SSG single-host logon
	SSG virtual path identifier/virtual channel identifier (VPI/VCI) RADIUS accounting
	Transparent passthrough
	Transparent passthrough filter
VPI/VCI static bind index to service profile (or vc service map)	
<b>Other</b>	CEF Switching
	L2TP access concentrator (LAC) CEF Switching

# New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 6400 NRP for Release 12.1(3) DC2.

**Note**

---

Most of the features documented in this section have a feature module. For information about feature modules, see the section “Feature Modules” on page 23.

---

## 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.

## 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 on 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 on 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 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

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.

## New Hardware Features Supported in Release 12.1(3) DC

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

## New Software Features in Release 12.1(3) DC

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

## 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 on 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 on 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 on CEF, see the chapter “Cisco Express Forwarding” in the *Cisco IOS Switching Services Configuration Guide*. For more information on L2TP, see the *Layer 2 Tunnel 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(3) DC works with the Cisco Service Selection Dashboard (SSD) version 2.2. To use the Single-Host Logon feature, you can install and configure Cisco SSD version 2.2S(1.12). However, note that both Cisco SSD version 2.2 and version 2.2S(1.12) have not completed a full-production release cycle and therefore are considered nonsupported software versions. Cisco SSD version 2.5(1) will be a fully supported production-release version that will also support Single-Host Logon, and is scheduled to be available in November 2000.

**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 on 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 on 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 Release 12.0(3) DC, while enhancements were added in later releases. Release 12.1(3) DC 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 on these enhancements, see the *Node Route Processor-Service Selection Gateway Enhancements IV* feature module.

## Important Notes

### Caveat CSCdr91706 and Cisco IOS HTTP Vulnerability

A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the Cisco IOS HTTP service is enabled, browsing to <http://router-ip/anytext?/> is attempted, and the enable password is supplied when requested. This defect can be exploited to produce a denial of service (DoS) attack.

The vulnerability, identified as Cisco bug ID CSCdr91706, affects virtually all mainstream Cisco routers and switches running Cisco IOS software releases 12.0 through 12.1, inclusive. This is not the same defect as CSCdr36952.

The vulnerability has been corrected and Cisco is making fixed releases available for free to replace all affected Cisco IOS releases. Customers are urged to upgrade to releases that are not vulnerable to this defect as shown in detail below.

This vulnerability can only be exploited if the enable password is known or not set.

You are strongly encouraged to read the complete advisory, which is available at <http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml>.

### DHCP for Unnumbered Interfaces Using RBE in Cisco IOS Release 12.1(3) DC2

After posting the images of Cisco IOS Release 12.1(3) DC2 to CCO, a problem was found with DHCP for unnumbered interfaces using RBE. Customers who are currently using this feature in Release 12.1(3) DC2 should not upgrade to Release 12.1(3) DC but should continue to use Release 12.1(3) DC2 until further notice. Images that integrate a fix for this problem are expected to be available soon.

## Session and Tunnel Scalability

Cisco IOS Release 12.1(3) DC2 supports the number of sessions and tunnels shown in Table 3. While using NRP-SSG, Cisco IOS Release 12.1(3) DC2 supports the number of sessions and tunnels shown in Table 4.

**Table 3** Session and Tunnel Scalability in Cisco IOS Release 12.1(3) DC2

Protocol	Number of Supported Sessions	Number of Supported Tunnels
L2TP PPPoA	up to 1700	up to 300
L2TP PPPoE	up to 2000	up to 300
L2TP Tunnel Switch PPPoA	up to 940	up to 50 Ingress up to 10 Egress
L2TP Tunnel Switch PPPoE	up to 940	up to 50 Ingress up to 10 Egress
PPPoA	up to 2000	—

**Table 3** Session and Tunnel Scalability in Cisco IOS Release 12.1(3) DC2

Protocol	Number of Supported Sessions	Number of Supported Tunnels
PPPoE	up to 2000	—
PPP Autosense	up to 2000	—
RBE	up to 2000	—
RFC 1483 IP Routed	up to 2000	—

**Table 4** NRP-SSG Session and Tunnel Scalability in Cisco IOS Release 12.1(3) DC2

Protocol with NRP-SSG	Number of Supported Sessions	Number of Supported Tunnels
L2TP PPPoA	up to 1000	up to 50
L2TP PPPoE	up to 1000	up to 50
PPPoA	up to 2000	—
PPPoE	up to 2000	—
RBE	up to 2000	—
RFC 1483 IP Routed	up to 2000	—

**Note**

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

## Software Caveats

Caveats describe unexpected behavior in the Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. This section contains open caveats for the current Cisco 6400 NRP IOS release only.

Caveats in Cisco IOS Release 12.1 T also apply to Release 12.1(3) DC2. For information on caveats in Cisco IOS Release 12.1 T, see *Caveats for Cisco IOS Release 12.1 T* located on CCO and the Documentation CD-ROM.

**Note**

If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II on CCO, click on **Technical Assistance Center**, then **Software Bug Toolkit**. 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(1) DC1

This section describes possibly unexpected behavior by Cisco IOS Release 12.1(1) DC1. This section describes severity 1, 2, and selected severity 3 caveats.

- 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 **atm ilmi-pvc-discovery subinterface** 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 **atm ilmi-pvc-discovery** 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.
- CSCdp86322
 

When an NRP-SSG subscriber exceeds the maximum number of services determined by the **ssg maxservice** global configuration command, the Cisco SSD incorrectly displays the following message: “The server returned an invalid or unrecognized response.”

The correct message reads: “You have reached the maximum allowed number of concurrently logged in services for your system, host-ID. Please logoff of at least one service, and try your service logon request again.”

Workaround: Click **OK** to recognize the error, and select the service on the viewService frame again. The correct message will appear.
- CSCdr36174
 

The NRP-SSG connection traffic counter always reads zero for the input direction. There is no workaround.
- 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
- CSCdr54934
 

The NRP runs out of memory with 2000 NRP-SSG PPPoE sessions using L2TP services. Current testing shows normal system behavior with 1000 NRP-SSG PPPoE sessions and 50 L2TP tunnels.
- CSCdr56756
 

The NRP-SSG DNS fault tolerance feature does not work while CEF is enabled. The secondary DNS sever becomes unreachable upon switchover.

Workaround: Disable CEF.
- 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.
- CSCds09497
 

Under extreme traffic loads in an NRP with Release 12.1(01) DC1 or a higher release, PPP sessions may fail to originate new sessions. Workaround: Restart the processor.

- CSCds21838  
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 requests 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.
- CSCds22721  
When SSG receives a service profile from a local AAA server, it receives a “V” or an “X”, both of which are attributes (service-information codes) for proxy service connections. SSG then forwards the “V” attribute as a secret cookie to the remote server, while the “X” attribute can be forwarded as a full username (that is, user@service) to the remote server. This allows differentiation in the RADIUS requests for processing.  
  
However, if the user initially logs in with a full username, the “X” attribute does not function and will not show in RADIUS debug messages. There is no workaround.
- 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.
- CSCds26968  
When IP relay is configured on an unnumbered VPN Routing/Forwarding (VRF) interface, the static route might be inserted into the global routing table instead of the VRF routing table. 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.

## Resolved Caveats—Release 12.1(3) DC2

This section describes caveats that have been closed and resolved in Cisco IOS Release 12.1(3) DC2.

- 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>

## Resolved Caveats—Release 12.1(3) DC1

This section describes caveats that have been closed and resolved in Cisco IOS Release 12.1(3) DC.1

- CSCdr36174  
The NRP-SSG connection traffic counter always reads zero for the input direction. There is no workaround.

- CSCdp42210  
A NRP ATM interface stops sending when there are multiple particles with data-length 0 at the last particle. The only way to exit this situation is to use the **shutdown** interface configuration command followed by the **no shut** interface configuration command. There is no workaround.
- CSCdr56756  
The NRP-SSG DNS fault tolerance feature does not work while CEF is enabled. The secondary DNS sever becomes unreachable upon switchover.  
Workaround: Disable CEF.

## Open Caveats—Release 12.1(3) DC

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

- CSCdp75605  
In a PPPoA configuration, if a Fast Ethernet interface runs out of local memory under heavy traffic, the pool-memory manager might not be able to allocate fallback pool memory fast enough. This might cause the Fast Ethernet interface to reset and reject incoming traffic temporarily.  
There is no workaround.
- CSCdp83066  
Repeated ATM interface flapping on the NRP combined with a high traffic load might cause the NRP to run out of heap memory and subsequently reload. This problem is seen with 880 sessions, 100 ingress tunnels and 10 egress tunnels. There is no workaround.
- CSCdr52400  
An NRP might occasionally stop transmitting packets on the virtual circuit. When issuing a **show controller atm 0/0/0** command, the queued counter will show 255, while the pxmt counter will show 0.  
Workaround: Delete the PVC and re-configure it.  
Alternative workaround: Issue a **shut** command followed by a **no shut** command on the interface with the VC.
- CSCdr91706 and Cisco IOS HTTP Vulnerability  
A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the Cisco IOS HTTP service is enabled, browsing to `http://router-ip/anytext?/` is attempted, and the enable password is supplied when requested. This defect can be exploited to produce a denial of service (DoS) attack.  
The vulnerability, identified as Cisco bug ID CSCdr91706, affects virtually all mainstream Cisco routers and switches running Cisco IOS software releases 12.0 through 12.1, inclusive. This is not the same defect as CSCdr36952.  
The vulnerability has been corrected and Cisco is making fixed releases available for free to replace all affected Cisco IOS releases. Customers are urged to upgrade to releases that are not vulnerable to this defect as shown in detail below.  
This vulnerability can only be exploited if the enable password is known or not set.  
You are strongly encouraged to read the complete advisory, which is available at <http://www.cisco.com/warp/public/707/ioshttpserverquery-pub.shtml>.

- CSCdr96500  
The content of “ConnectionObject” of the SSG web-selection L2TP service shows no traffic statistics for both the input and output. There is no workaround.
- CSCds02872  
If fast-switching is turned on, the route bridge encapsulation (RBE) feature does not pad frames with a size less than the minimum Ethernet size to the required minimum IEEE 802.3 frame size. If the remote site on the receiving end does not pad the frames, they will be dropped as runt frames (that is, frames that are smaller than the minimum IEEE 802.3 frame size).  
Workaround: Turn off fast-switching on the ATM interface.
- CSCds07667  
In a PPPoA configuration, an NRP with SSG enabled might reload due to multiple spurious accesses in the PPP manager. There is no workaround.
- CSCds12380  
An NRP with SSG enabled might reload due to a red-zone violation.  
Workaround: Disable SSG.
- CSCds12783  
An NRP with SSG enabled might reload when an IP address that is assigned to a PPP session is also assigned to a second PPP session before the first PPP session has been completed.  
Workaround: Always assign the same IP address to a user by statically configuring the IP address in the RADIUS server or the NRP.
- CSCds31877  
When issuing the command **clear int virtual-access** on a virtual-access interface one would expect the PPP session to be terminated. This is not the case as the command has no effect.  
Workaround: Clear or delete and recreate the source interface (ATM VC).

## Resolved Caveats—Release 12.1(3) DC

This section describes caveats that have been closed and resolved in Cisco IOS Release 12.1(3) DC.

- CSCdr42062  
When MLP is enabled on an L2TP Network Server (LNS) and a PPP client, the dial-out feature of L2TP causes packets to be dropped. There is no workaround.
- CSCdr59508  
In a system with a lot of VCs configured (for example, 2000), if the ATM VC TX ring size is set to a value larger than its default value of 32 (for example, 128) and the Fast Ethernet interface experiences heavy traffic, malloc will fail, which causes the Fast Ethernet interface to reset.  
Workaround: Set the ATM VC TX ring-size to its default value of 32, using the **atm vc tx 32** command. If a lot of VCs are configured, the ATM VC TX ring size should not be set to a value higher than its default.
- CSCdr61340  
The NRP crashes during reload when both of the following conditions are met:
  - NRP-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.
- CSCdr87393
 

Under heavy traffic on the ATM interface, frequent CLI operations that reset the ATM interface (for example, the CLI command **clear int atm0/0/0**) may cause a bus-error reload in the NRP. There is no workaround.
- CSCdr97361
 

The execution of the **Show ip nat translation verbose** may cause the 6400 NRP to reload.  
Workaround: Set the terminal length to “term len 0” before executing the **Show ip nat translation verbose**.
- CSCds16400
 

The packet processing of the NAT code handling H.245 might be leaking memory under one of the following error conditions:

  - when an H245 message processed by the NAT can not be properly encoded back by the Operations Support System (OSS) libraries, or
  - when the encoding buffer cannot be freed by the OSS, or
  - when the NAT, under a stress condition, is out of global ports, or
  - when the NAT can not allocate memory (because of a chain reaction).

There is no workaround.

## Preexisting NRP Hardware Caveats

This section describes possible unexpected behavior by earlier hardware versions of the NRP. To determine your NRP part number (P/N), see the “Determining Your NRP Part Number” on page 20.

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

Affected Part Number: 800-03785-03

Symptom:  
While the NSP is in Slot 0A of a single NSP system, the NRPs 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 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 boots the first image in Flash memory after a reset. This problem occurs after one of the following actions:

  - NRP 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:

- a. Enter **delete flash:\*** to mark all files on the Flash memory device for deletion.
- b. Enter **squeeze flash:** to permanently erase all files marked for deletion.
- c. Use the **copy flash: EXEC** command to copy the desired image to the Flash memory device.
- d. 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 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, the NRP does not ignore the **boot system** global configuration command entries in the startup configuration.

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

**Affected Part Numbers:**

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

**Symptoms:**

With or without redundancy configured, an NRP inserted into a live system might reset the NRP in the adjacent slot of the slot pair. NRP 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 redundancy and your system contains four or fewer NRPs, place only one NRP in each slot pair.
  - If this workaround is not feasible, replace your NRP(s) with P/N 800-03655-07 or higher.
- CSCdr08888—NRP 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 console, the NRP console port does not respond.

**Workaround:**

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

- CSCdr16154—NRP 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 NRPs.

**Workaround (use one of the following):**

- Reduce the number of NRPs in the system
  - Make sure all the NRPs are P/N 800-03655-09 or higher
  - Make sure the NSP is P/N 800-03785-08 or higher.
- CSCdr61340
- The NRP crashes during reload when both of the following conditions are met:

- NRP-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, disable the SSG with the **no ssg enable** command.

- CSCdr97361

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

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

## Determining Your NRP Part Number

To determine the NRP part number, use one of the following methods with the information in Table 5:

- If you are holding the board, look at the 800- part number label on the back of the NRP.
- If you can only view the faceplate of the NRP, 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 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 5 NRP Part Numbers**

CLEI Code	800- Part Number	73- Part Number
BAC5EEPDAA	800-03655-01	73-3082-03
BAC5EEPDAB	800-03655-02	73-3082-04
BAC5EEPDAC	800-03655-03	73-3082-05

**Table 5** NRP Part Numbers

CLEI Code	800- Part Number	73- Part Number
BAC5EEPDA D	800-03655-04	73-3082-06
BAC5EEPDAE	800-03655-05	73-3082-07
BAC5EEPDAF	800-03655-06	73-3082-08
BAC7RUBCAA	800-03655-07	73-3082-09
BAC7RUBCAB	800-03655-08	73-3082-10
BAC7VUBCAA	800-03655-09	73-3082-11

## Related Documentation

The following sections describe the documentation available for the Cisco 6400 universal access concentrator. The most up-to-date documentation can be found on the Web via Cisco Connection Online (CCO) and on the Documentation CD-ROM. These electronic documents might contain updates and modifications made after the hard-copy documents were printed.

These release notes should be used in conjunction with the documents listed in the following sections:

- Release-Specific Documents, page 21
- Platform-Specific Documents, page 21
- Feature Modules, page 23
- Cisco IOS Software Documentation Set, page 23

## Release-Specific Documents

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

- *Cross-Platform Release Notes*

On CCO 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 CCO at:

**Technical Documents**

## Platform-Specific Documents

The documents listed in Table 6 are available for the Cisco 6400 UAC on CCO and the Documentation CD-ROM.

To access Cisco 6400 documentation on CCO, 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 6 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"> <li>About This Manual</li> <li>Hardware Description</li> <li>Preparing for Installation</li> <li>Installing the Cisco 6400</li> <li>Troubleshooting</li> <li>Maintaining the Cisco 6400</li> <li>System Specifications</li> <li>Glossary</li> <li>Configuration Worksheets</li> <li>Installing the AC-Input Power Shelf and Power Supply</li> </ul>
<i>Cisco 6400 UAC Site Planning Guide</i>	<ul style="list-style-type: none"> <li>About This Guide</li> <li>Cisco 6400 Overview</li> <li>Site Planning Considerations</li> <li>System Specifications</li> <li>Cabling Specifications</li> <li>Glossary</li> </ul>
<i>Regulatory Compliance and Safety Information for the Cisco 6400</i>	<ul style="list-style-type: none"> <li>Overview of the Cisco 6400 Universal Access Concentrator</li> <li>General Documentation Information</li> <li>Agency Approvals</li> <li>Translated Safety Warnings</li> <li>Cisco Connection Online</li> </ul>
<i>Cisco 6400 UAC Software Configuration Guide and Command Reference</i>	<ul style="list-style-type: none"> <li>About This Guide</li> <li>Product Overview and Configuration</li> <li>Cisco IOS Software Fundamentals</li> <li>Using the Web Console</li> <li>Configuring the NSP</li> <li>Configuring System Features</li> <li>Configuring the NRP</li> <li>Configuring Interfaces</li> <li>Command Reference</li> <li>MIB Information</li> <li>Resolving Error Messages</li> <li>Glossary</li> </ul>

**Table 6** Platform Documents for the Cisco 6400 Universal Access Concentrator

Document Title	Chapter Topics
<i>Cisco 6400 FRU Installation and Replacement</i>	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 CCO 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 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 that are 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 two books: a configuration guide and a corresponding command reference. 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 CCO and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

On CCO 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

Table 7 describes 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 CCO and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On CCO 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 7 Cisco IOS Software Release 12.1 Documentation Set**

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

**Table 7 Cisco IOS Software Release 12.1 Documentation Set (continued)**

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Dial Services Configuration Guide: Terminal Services</i></li> <li>• <i>Cisco IOS Dial Services Configuration Guide: Network Services</i></li> <li>• <i>Cisco IOS Dial Services Command Reference</i></li> </ul>	Preparing for Dial Access Modem Configuration and Management ISDN and Signalling 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"> <li>• <i>Cisco IOS Interface Configuration Guide</i></li> <li>• <i>Cisco IOS Interface Command Reference</i></li> </ul>	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces
<ul style="list-style-type: none"> <li>• <i>Cisco IOS IP and IP Routing Configuration Guide</i></li> <li>• <i>Cisco IOS IP and IP Routing Command Reference</i></li> </ul>	IP Overview IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> <li>• <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i></li> <li>• <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i></li> </ul>	AppleTalk and Novell IPX Overview Configuring AppleTalk Configuring Novell IPX
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i></li> <li>• <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i></li> </ul>	Overview Configuring Apollo Domain Configuring Banyan VINES Configuring DECnet Configuring ISO CLNS Configuring XNS
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Multiservice Applications Configuration Guide</i></li> <li>• <i>Cisco IOS Multiservice Applications Command Reference</i></li> </ul>	Multiservice Applications Overview Voice Video Broadband
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Quality of Service Solutions Configuration Guide</i></li> <li>• <i>Cisco IOS Quality of Service Solutions Command Reference</i></li> </ul>	Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping Signalling Link Efficiency Mechanisms Quality of Service Solutions

**Table 7 Cisco IOS Software Release 12.1 Documentation Set (continued)**

Books	Major Topics
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Configuration Guide</i></li> <li>• <i>Cisco IOS Security Command Reference</i></li> </ul>	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"> <li>• <i>Cisco IOS Switching Services Configuration Guide</i></li> <li>• <i>Cisco IOS Switching Services Command Reference</i></li> </ul>	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"> <li>• <i>Cisco IOS Wide-Area Networking Configuration Guide</i></li> <li>• <i>Cisco IOS Wide-Area Networking Command Reference</i></li> </ul>	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"> <li>• <i>Cisco IOS Configuration Master Index</i></li> <li>• <i>Cisco IOS Command Reference Master Index</i></li> <li>• <i>Cisco IOS Debug Command Reference</i></li> <li>• <i>Cisco IOS Dial Services Quick Configuration Guide</i></li> <li>• <i>Cisco IOS Software System Error Messages</i></li> <li>• <i>Cisco IOS Configuration Guide Master Index</i></li> <li>• <i>New Features in 12.1-Based Limited Lifetime Releases</i></li> <li>• <i>New Features in Release 12.1 T</i></li> <li>• Release Notes (Release note and caveat documentation for 12.1-based releases and various platforms)</li> </ul>	



**Note**

*Cisco Management Information Base (MIB) User Quick Reference* is no longer published. For the latest list of MIBs supported by Cisco, see the *Cisco Network Management Toolkit* on CCO: **Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB.**

# Obtaining Documentation

## World Wide Web

You can access the most current Cisco documentation on the World Wide Web at <http://www.cisco.com>. Translated documentation can be accessed at [http://www.cisco.com/public/countries\\_languages.shtml](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. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

## Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at <http://www.cisco.com/cgi-bin/subcat/kaojump.cgi>.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

# Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the Web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

## Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online 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.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, 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 CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: [www.cisco.com](http://www.cisco.com)
- Telnet: [cco.cisco.com](http://cco.cisco.com)
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to [cco-team@cisco.com](mailto:cco-team@cisco.com).

## Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use [www.cisco.com/techsupport](http://www.cisco.com/techsupport).

To contact TAC by e-mail, use one of the following:

Language	E-mail Address
English	<a href="mailto:tac@cisco.com">tac@cisco.com</a>
Hanzi (Chinese)	<a href="mailto:chinese-tac@cisco.com">chinese-tac@cisco.com</a>
Kanji (Japanese)	<a href="mailto:japan-tac@cisco.com">japan-tac@cisco.com</a>
Hangul (Korean)	<a href="mailto:korea-tac@cisco.com">korea-tac@cisco.com</a>
Spanish	<a href="mailto:tac@cisco.com">tac@cisco.com</a>
Thai	<a href="mailto:thai-tac@cisco.com">thai-tac@cisco.com</a>

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site:  
<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

## Software Configuration Tips on the Cisco Technical Assistance Center Home Page

If you have a CCO log-in account, you can access the following URL, which contains links and tips on configuring your Cisco products:

[http://www.cisco.com/kobayashi/technotes/serv\\_tips.shtml](http://www.cisco.com/kobayashi/technotes/serv_tips.shtml)

This URL is subject to change without notice. If it changes, point your Web browser to CCO, press **Login**, and click on this path: **Technical Assistance Center: Technical Tips**.

The following sections are provided from the Technical Tips page:

- Access Dial Cookbook—Contains common configurations or recipes for configuring various access routes and dial technologies.

- **Field Notices**—Notifies you of any critical issues regarding Cisco products and includes problem descriptions, safety or security issues, and hardware defects.
- **Frequently Asked Questions**—Describes the most frequently asked technical questions about Cisco hardware and software.
- **Hardware**—Provides technical tips related to specific hardware platforms.
- **Hot Tips**—Describes popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888 50-CISCO (888 502-4726). From other areas, call 650 596-4408.
- **Internetworking Features**—Lists tips on using Cisco IOS software features and services.
- **Sample Configurations**—Provides actual configuration examples that are complete with topology and annotations.

## 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](mailto: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 and value your comments.

---

This document is to be used in conjunction with the documents listed in the “Related Documentation” section on page 21

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 © 2000–2002, Cisco Systems, Inc.  
All rights reserved.