



Cisco 6400 NSP – Release Notes for Cisco IOS Release 12.1(5)DB

February 16, 2002



Note

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

These release notes for the Cisco 6400 node switch processor (NSP) describe the enhancements provided in Cisco IOS Release 12.1(5)DB1. These release notes are updated as needed.

For a list of the software caveats that apply to Release 12.1(5)DB1, see the [“Preexisting NSP Hardware Caveats” section on page 17](#) 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.

Contents

These release notes describe the following topics:

- [System Requirements, page 2](#)
- [New and Changed Information, page 6](#)
- [Important Notes, page 9](#)
- [Software Caveats, page 11](#)
- [Preexisting NSP Hardware Caveats, page 17](#)
- [Related Documentation, page 19](#)
- [Obtaining Documentation, page 25](#)
- [Obtaining Technical Assistance, page 26](#)



System Requirements

This section describes the system requirements for Cisco IOS Release 12.1(5)DB1 and includes the following sections:

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

Memory Recommendations

Table 1 lists the memory recommendations for the NSP.

Table 1 *Memory Recommendations for the Cisco 6400 NSP*

Product Name	Image Names	Recommended Main Memory	Recommended Flash Memory
Cisco 6400 Series IOS FOR NSP	c6400s-wp-mz c6400s-html.tar	The standard 64 MB DRAM memory configuration supports up to 12K virtual circuits (VCs). 128 MB DRAM is recommended for supporting up to 32K VCs, or for using ATM RMON or ATM Accounting. 128 MB DRAM is also recommended for an upgrade from an earlier release to Cisco IOS Release 12.1(5)DB1.	20 MB or 32 MB ¹ 350 MB is recommended for NRP-2 configurations

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

Supported Hardware

Cisco IOS Release 12.1(5)DB1 supports the Cisco 6400 NSP and the NSP with Stratum 3/BITS (NSP-S3B). The NSP-S3B, otherwise identical to the NSP, is required to use the Building Integrated Timing Supply (BITS) Network Clocking software feature. For detailed descriptions of the new hardware features, see the [“New and Changed Information” section on page 6](#) and the [“Related Documentation” section on page 19](#).

Software Compatibility

Cisco recommends that Cisco IOS Release 12.1(5)DB1 be used concurrently with Cisco IOS Release 12.1(5)DC for the Cisco 6400 node route processor (NRP). For information about Release 12.1(5)DC for the NRP, see the *Release Notes for Cisco 6400 Node Route Processor (NRP) for Cisco IOS Release 12.1(5)DC*.

Determining the Software Version

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

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) C6400 Software (C6400S-WP-M), Version 12.1(5)DB1, 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-NSP system to a new software release, see the software note *Upgrading Software on the 6400 UAC* located at http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/6400/softnote/upgradsw.htm

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

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

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

This product bulletin does not contain information specific to Cisco IOS Release 12.1 DB1 but provides generic upgrade information that may apply to Cisco IOS Release 12.1 DB1.

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 NSP image called c6400s-wp-mz 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. If you have a Cisco.com login account, you can find image and release information regarding features prior to Cisco IOS Release 12.1(5)DB1 by using the Feature Navigator tool at <http://www.cisco.com/go/fn>.

Table 2 Features Supported by the Cisco 6400 NSP in Cisco IOS Release 12.1(5)DC

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

Table 2 *Features Supported by the Cisco 6400 NSP in Cisco IOS Release 12.1(5)DC (continued)*

Feature	Supported as of Cisco IOS Release
Shaped CBR VP tunnels (up to 128)	12.0(4)DB
Substitution of other service categories in shaped VP tunnels	12.0(4)DB
Support for non-zero MCR on ABR connections	12.0(4)DB
Unspecified bit rate (UBR)	12.0(4)DB
UBR + MCR	12.0(4)DB
Variable bit rate-non-real time (VBR-NRT)	12.0(4)DB
VBR-real time (RT)	12.0(4)DB
Configuration and Monitoring	
ATM access lists on Interim Local Management Interface (ILMI) registration	12.0(4)DB
ATM soft restart	12.0(4)DB
PCMCIA ³ Disk Mirroring	12.1(5)DB
Per-VC or per-VP nondisruptive port snooping	12.0(4)DB
Hardware Support	
1+1 Slot Redundancy (EHSA ⁴)	12.0(4)DB
Network Management Ethernet (NME)	12.0(5)DB
NRP-2 support	12.1(4)DB
NSP 1+1 Redundancy	12.0(4)DB
Synchronous Optical Network (SONET) automatic protection switching (APS) support	12.0(4)DB
Stratum 3/BITS	12.0(7)DB
Telco alarms	12.0(4)DB
IP and Routing	
Dynamic Host Configuration Protocol (DHCP) client support	12.0(4)DB
Internet Protocol (IP)	12.0(4)DB
Network Time Protocol (NTP)	12.0(4)DB
Telnet	12.0(4)DB
Network Management	
ATM accounting enhancements	12.0(4)DB
ATM Accounting Management Information Base (MIB)	12.0(4)DB
ATM remote monitoring (RMON) MIB	12.0(4)DB
Signaling diagnostics and MIB	12.0(4)DB
Simple Network Management Protocol (SNMP)	12.0(4)DB
Web Console	12.0(4)DB
RADIUS/AAA	
Terminal Access Controller Access Control System Plus (TACACS+) (admin login only)	12.0(4)DB

Table 2 *Features Supported by the Cisco 6400 NSP in Cisco IOS Release 12.1(5)DC (continued)*

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

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

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 6400 NSP for Release 12.1(5) DB1.

New Features in Release 12.1(5)DB1

There are no new features in Cisco IOS Release 12.1(5)DB1

New Features in Release 12.1(5)DB

PCMCIA Disk Mirroring

The PCMCIA disk mirroring feature enables automatic data synchronization between the PCMCIA disks of two redundant Cisco 6400 NSPs. Disk synchronization is the act of copying data from one disk to another.

The NRP-2 has no local image or file storage. The NSP stores the following NRP-2 files on the PCMCIA disk installed in disk slot 0: software images, startup configurations, ROM state information, and crash information.

Before the support of disk mirroring, NRP-2 support was not seamless after an NSP failover and could have required operator intervention to restore the NRP-2 to its state before the NSP failover. Now the NRP-2 will have continued support from the NSP, except during the relatively short NSP failover period.

PCMCIA disk mirroring is enabled by default, and disk synchronization is initiated each time one of the following events occurs:

- The primary or secondary NSP boots or reloads
- The secondary NSP is inserted into the Cisco 6400 chassis
- A PCMCIA disk is inserted into disk slot 0 of the primary or secondary NSP
- The PCMCIA disk in disk slot 0 of either NSP is formatted
- A command is entered to perform any of the following:
 - Reenable disk mirroring (**mirror**)
 - Explicitly synchronize the disks (**redundancy sync**)
 - Modify or reorganize the files on the disks (**copy, rename, erase, delete, mkdir, format**)

For more information about the PCMCIA disk mirroring feature, see the *PCMCIA Disk Mirroring* feature module.

New Features in Release 12.1(4)DB1

NRP-2 Support

The NSP provides support for the second-generation node route processor (NRP-2) for the Cisco 6400 platform, which is introduced in Cisco IOS Release 12.1(4) DC.

The NSP performs the following functions for the NRP-2:

- Switching of incoming virtual paths (VPs) to the appropriate NRP-2.
- Controlling of configuration storage, console traffic, and network management. This provides 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.

The NSP also supports the NRP-1, but does not perform the above-mentioned functions for the NRP-1. These functions are performed by the NRP-1 itself. [Table 3](#) lists the functions that the NSP performs for the NRP-2 and shows how the NRP-1 performs these functions.

Table 3 NSP Support for the NRP-2 in Comparison to the NRP-1

Characteristic	Supported by NSP for NRP-2	Supported by NRP-1
Location of software images, configurations, and crash information	PCMCIA disk on NSP	NRP-1 memory (built-in or internal Flash)
Message logging	NRP-2 messages are logged on both the NSP and NRP-2. NRP-2 messages on the NSP include the NRP-2 slot number.	Messages are logged on the NRP-1 as local messages.
Console line access	Indirect external connection via the NSP. NSP contains a virtual communication server to access the NRP-2 console.	Direct external connection to NRP-1 console port or auxiliary port
ROMMON ¹	NRP-2 ROM state information is stored on the NSP PCMCIA disk.	NRP-1 ROM state information stored locally on NRP-1
SNMP ²	Standard SNMP services	Standard SNMP services, or can use the NSP as the proxy forwarder

1. ROMMON = ROM Monitor

2. SNMP = Simple Network Management Protocol

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

Input Translation Table Enhancements

This software feature adds three enhancements that display and alter switch behavior in managing the input translation table (ITT) resource.

The ITT is a hardware data structure used in the NSP for handling the incoming cells. It consists of entries that, for virtual circuit (VC) switching, are allocated in contiguous blocks, while each block is dedicated to a virtual path identifier (VPI) on an interface. Each entry specifies whether a virtual channel identifier (VCI) is valid within a VPI. The allocated blocks must be a power of two in sizes such as 16, 32, 64, and so on. The ITT is used only when both interfaces that the VC transits through are up.

The NSP has a single ITT, organized in two banks of 32K entries each. When a VC is created, a block of entries is allocated in the ITT for that VPI. The block size should be a power of two that is greater than or equal to the VCI value. This limits the use of large VCI values and also the distribution of VCIs on VPIs as the number of VCs approaches 32K. When an additional VC is added to a VPI that requires a larger block size than the current block, the current block is copied to a new larger block, and the original block is freed. This leaves a series of small-sized blocks that are unused. ITT memory is fragmented due to this growing technique.

In Release 12.1(4)DB1, the NSP has the following three new functions:

- Fragmentation minimization
New configuration commands to minimize fragmentation enable the NSP to automatically determine the minimum ITT block size needed to support the PVCs configured for each interface and VPI. When an interface comes up, the **minblock** command specifies the ITT block size requested for a VPI on that interface.

- ITT block shrinking
By default, the ITT blocks grow as necessary to accommodate high VCI values for a given port VPI, but ITT space is not returned unless the entire ITT block is free. A new command is introduced that reduces the size of an ITT block when a VC with a high-numbered VCI is deleted.
- Capability to view used/unused ITT blocks
A command to display details of the used and unused ITT blocks is also added. This gives a picture of the quantity and quality of ITT utilization at a given time. The output of the **show** command allows you to view details of the free blocks by size and bank, the aggregate free space left, and the location of blocks that are in use.

**Note**

The new configuration commands for this feature require additional processing, which slightly reduces call setup rates and slightly increases memory usage when the modes are enabled.

For more information, see the *Input Translation Table Management Enhancements* feature module.

No New Features in Release 12.1(3)DB

There are no new features in Cisco IOS Release 12.1(3)DB

No New Features in Release 12.1(1)DB1

There are no new features in Cisco IOS Release 12.1(1)DB1

Important Notes

The following sections contain important information about the use of your Cisco 6400 UAC NSP.

ATM Generic Flow Control Field

When an ATM cell is received on the NSP, the generic flow control (GFC) field of the ATM cell is passed without modification to the outbound virtual circuit. This is not compliant with the ATM Forum UNI specification, version 3.1, which requires all bits of the GCF field to be reset to zero.

NSP Disk Backup

The Cisco IOS disk file system is based on the DOS ATA file system. As with DOS Windows systems, the contents of the disk might become corrupted with improper system shutdown. Make sure to back up the contents of your NSP disk to avoid data loss.

Backups can be made to a second flash disk in your primary NSP, to a flash disk in your secondary NSP, or to an off-system server (via FTP, TFTP, or RCP).

If the flash disk does become corrupted, there are two recovery options:

- Remove the disk, install it in a laptop PC, and run **chkdsk** on the disk.
- Reformat the disk in Cisco IOS and restore the data from your backup source.

Session Scalability Commands

Table 4 lists VP switching session scalability commands with recommended settings that apply to the NSP in Cisco IOS Release 12.1(4)DB1.

Table 4 VP Switching Session Scalability Commands with Recommended Settings for the NSP

Configuration Task and Commands	Guidelines
<p>Setting the EFCI and ABR Marking Threshold: NSP(config)# atm threshold-group <i>number</i> marking-threshold <i>pct</i></p>	<p>1. Purpose Specifies the threshold at which the per-connection queue is considered full for EFCI¹ marking and ABR² relative-rate marking.</p> <p>2. Symptoms Use when the threshold group becomes congested (the cumulative number of cells on the queues of VCs in the threshold group approaches the configured max-cells value) and the maximum number of cells per queue shrinks from the threshold group max-queue-limit to the min-queue-limit. As the queue size changes, the marking threshold changes, and the installed threshold is made as close as possible to the percent of queue-full specified.</p> <p>3. Recommended Settings To achieve a large number of sessions, Cisco recommends a setting of 80% on the NSP.</p>
<p>Setting the Largest per-VC Queue Limit: NSP(config)# atm threshold-group <i>number</i> max-queue-limit <i>cells</i></p>	<p>1. Purpose Specifies the largest per-VC queue limit for a specified threshold group.</p> <p>2. Symptoms Use when the threshold group becomes congested (the cumulative number of cells on the queues of the VCs in the threshold group approaches the configured max-cells value) and the maximum number of cells per queue shrinks from the threshold group max-queue-limit to the min-queue-limit.</p> <p>3. Recommended Settings To achieve a large number of sessions, Cisco recommends a setting of 16,383 (that is, the value for <i>cells</i>) on the NSP.</p>
<p>Setting the Smallest per-VC Queue Limit: NSP(config)# atm threshold-group <i>number</i> min-queue-limit <i>cells</i></p>	<p>1. Purpose Specifies the smallest per-VC queue limit for a specified threshold group.</p> <p>2. Symptoms Use when the threshold group becomes congested (the cumulative number of cells on the queues of VCs in the threshold group approaches the configured max-cells value) and the maximum number of cells per-queue shrinks from the threshold group max-queue-limit to the min-queue-limit.</p> <p>3. Recommended Settings To achieve a large number of sessions, Cisco recommends a setting of 1023 (that is, the value for <i>cells</i>) on the NSP.</p>

- 1. EFCI = explicit forward congestion indication
- 2. ABR = Available Bit Rate

Using Verbose Debug Options

On a dual-NSP system, switchovers can occur if verbose debugging commands, such as **debug all** or **debug oir** commands, are used. To avoid this situation when using verbose **debug** commands, execute the **redundancy keepalive disable** command at the EXEC prompt prior to turning on the **debug** command. After debugging is disabled, enter the **redundancy keepalive enable** command to restore normal system operation.

Web Console Issues

The Web Console application is designed to use JavaScript, which is available with both Netscape Navigator and Microsoft Internet Explorer. However, a number of issues are present when using either application. To date, using Netscape Navigator 4.x has resulted in fewer issues than Microsoft Internet Explorer 4.x.

Before using the Web Console application, verify that your browser is set to use at least 4 MB (4096 KB) of cache memory.

The following sections tell how to deal with some of the browser issues affecting each application.

Microsoft Internet Explorer 4.x

Web Console might not reflect the most current redundancy status and autosynchronization setting because the check box and option buttons are not displayed properly. Therefore, you must verify your configuration by viewing the configuration file.

An empty dialog box might display after you apply new settings in any of the Web Console pages. If an empty dialog box is displayed, click the Internet Explorer **Refresh** button to view your new settings.

The **show interface** command on the Status page fails with Internet Explorer. There is no workaround, so this function is not available.

Netscape Navigator 4.x

If a blank window is displayed after you resize your Navigator window, click the **Reload** button to redisplay the page. Frequent and rapid clicking on the Web Console Status page can cause syntax and LED errors. This problem is eliminated if the browser cache is set to 4096 KB.

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)DB1.

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)DB1 is in synchronization with Cisco IOS Release 12.1(5)T4.

This section contains open caveats for the current Cisco 6400 NSP Cisco IOS release only and includes severity 1, severity 2, and select severity 3 and severity 4 caveats (severity 4 caveats are minor 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. To reach Bug Navigator II, go to Cisco.com and press **Login**. Then go to **Software Center: Cisco IOS Software: Cisco Bugtool Navigator II**. Another option is to go to <http://www.cisco.com/support/bugtools/>.

Open Caveats—Release 12.1(5)DB1

There are no open caveats specific to Cisco IOS Release 12.1(5)DB1 that require documentation in the release notes.

Closed and Resolved Caveats—Release 12.1(5)DB1

This section describes caveats that have been closed and resolved in Cisco IOS Release 12.1(5)DB1.

- 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)DB

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

- 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.

- CSCdr65451

The Interim Local Management Interface cannot be brought up on DS3 interfaces. This causes the interfaces on a Cisco 6400 NSP to stay in the User-Network Interface. If the Cisco 6400 connects to a Cisco LightStream 1010, the Private Network Node Interface will never come up.

Workaround: Configure a well-known VC manually.

- 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.

- 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.

- CSCds24164

After inserting an NRP-2 into the Cisco 6400 chassis, the NSP console will stall for 10 to 30 seconds. The NSP prevents user input and stalls preexisting user input in order to assure internal data consistency and to properly bring the NRP-2 card online. There is no workaround.

- CSCds51415

During a power-on condition, if an NRP-2 is in a lower-numbered slot than an NRP-1, the user might see the following message on the NRP-1 console and the NRP-1 might reboot:

```
platform_interface_init: PAM mailbox Config not valid yet, pausing before re-reading
```

The NRP-1 will then boot correctly. There is no workaround.

- CSCds61145

When the **atm snoop** command is enabled on a Cisco 6400, issuing a **shutdown** command on the interface which has been configured with the **atm snoop** command might cause some cells to drop from the interface that is being snooped (that is, being monitored).

For example, if the command **atm snoop** is enabled on the “atm1/0/0” interface to monitor the “atm1/0/1” interface and the “atm1/0/0” interface is shutdown, some cells might be dropped from interface “atm1/0/1.” There is no other workaround than to keep the snooping interface always active.

- CSCdt29127

Upon NSP switchover, the Interim Local Management Interface (ILMI) will not come up on the CPU port of the newly active NSP.

Workaround: Reload both NSPs simultaneously.

- CSCdt32757
 Facility alarms from the NRP might not be correctly reported when the NSP fails over from primary to secondary.
 Workaround: issue a **hw-module slot x reset** command, where “x” is the slot in which the NRP is installed.
- CSCdt33730
 Performing port scans on a Cisco 6400 may cause “ALIGN-3-READEXCEPTION” messages on the console. There is no workaround to prevent these messages.
 If the volume of these messages is too high, the NSP might become unresponsive to the console for up to 20 seconds, as the Cisco IOS software ensures that all messages are forwarded to the serial console. During this time, you cannot Telnet or ping the router, nor make a connection through the console port. This is standard Cisco IOS software behavior during the process of forwarding messages to the serial console.
 Workaround: Configure the console logging rate as limiting, or issue the **no logging console** command.
- CSCdt41423
 A secondary NSP might pause indefinitely during a forced failover. This problem appears to be related to the disk. There is no workaround.
- CSCdt46373 and CSCdt45629
 Under stress scenarios in which a high number (>1000) of Tag Virtual Circuits (TVCs) is set up on an interface, some TVCs might not be set up successfully and the following message is printed:

```
%TCATM-4-RESOURCE_LIMIT: VC resource exhausted (for the interface that is used)
```

 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.
- 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.
- CSCdt71049
 An NSP OC-12 interface is configured for unidirectional automatic protection switching (APS). If the working, transmit side on a Cisco 6400 is disconnected, the NSP switches over to the protect side. This is bidirectional APS behavior and is contrary to the GR-253-CORE Telcordia specification. Although there is no workaround, this is not a service-impacting issue.

- CSCdt71080
An NSP OC12 interface is configured for unidirectional APS. If the protect side is non-functional, the user can still initiate a forced switch from the working side to the protect side. This is contrary to the GR-253-CORE Telcordia specification.
Workaround: Before initiating a forced switch from the working side, manually verify the integrity of the protect side, using the **show aps** command.
- CSCdt76617
PVCs on an NSP subinterface stops passing traffic after a reload or failover.
Workaround: Delete and re-add the PVCs.

Closed and Resolved Caveats—Release 12.1(5)DB

This section describes caveats that have been closed and resolved in Cisco IOS Release 12.1(5)DB.

- 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)DB.
- 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 DDTS 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)DB1.

- CSCds27879, CSCds67665, and CSCds68004

If the NRP-2 is reset or loses power while the configuration is being saved to a storage medium, the configuration file might become corrupted. Attempting to restart the NRP-2 might cause the NRP-2 to reload unexpectedly.

Workaround: Do not reset the NRP-2 after issuing a command that saves the configuration file, but wait until the saving process has been completed.

If the problem occurs due to a power loss or an accident, the storage medium needs to be formatted after the NRP-2 has been rebooted. Formatting the storage medium causes all data on the storage medium to be lost. If possible, before starting the formatting process, copy the data on the storage medium that needs to be formatted to another storage medium. When the formatting process has been completed, copy the data back to the storage medium that has been formatted and restore the corrupt configuration file from a backup copy.

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

- 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)DB and CSCds32217 was already resolved in Cisco IOS Release 12.1(4)DB1.

- CSCds73398

When removing the disk from the secondary NSP, the alarm LEDs are activated on that secondary NSP. The LEDs should remain unlit. There is no workaround.

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

- CSCdt56518

A Cisco NSP might drop cells when processing traffic at full line rate on an OC-3 interface. There is no workaround.

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

Preexisting NSP Hardware Caveats

This section describes possible unexpected behavior by earlier hardware versions of the NSP. To determine your NSP part number (P/N) and hardware version, see the “[Determining Your NSP Part Number and Hardware Version](#)” section on page 18.

- 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.

- CSCdk55268—After a bus error, the system does not reboot with autoboot enabled.

Affected Part Number:

800-03785-03

Symptom:

The system remains at the ROMMON prompt after a crash instead of rebooting automatically.

Workaround:

To prevent this problem, set the config register boot field to 0x2.

If the workaround does not work, replace the NSP with P/N 800-03785-04 or higher.

- CSCdm55885—NSPs might experience dropped cells.

A small percentage of NSPs might experience dropped cells. To determine if your NSP is affected, use the **show controllers atm 0/0/0 EXEC** command and check the values in the TPE column.

This field counts the number of transmit parity errors and should display all zeros for a good system. If a non-zero value is displayed in the TPE column, replace the NSP with P/N 800-03785-05 or higher.

- CSCdm78716—NME cable consolidation feature hardware requirement.

Affected Part Numbers:

800-03785-03 (without Deviation D99-3628), 800-03785-04, 800-03785-05

Symptoms:

The NSP’s network management Ethernet (NME) interface might lock up and require a reset with a “shut” and “no shut” sequence or a complete board reset.

The NSP might crash with a "Write Exception," "Bus Exception," or "System Reserved Exception" error message.

Because these symptoms might be caused by other problems, use the following table to determine the likelihood of this particular problem:

NME Cable Consolidation is Enabled?	System Uses Redundant NSPs?	Likelihood that CSCdm78716 is the Cause of the Problems
No	No	Not possible—no backplane Ethernet traffic to the NSPs
No	Yes	Possible, but unlikely
Yes	Yes or No	Likely

Workaround:

If you experience this problem, replace your NSP with P/N 800-03785-06 or higher, or with P/N 800-03785-03 with deviation sticker D99-3628 applied.

- CSCdr16154—NRP unrecognized card type.

Affected Part Numbers:

800-03785-01, 800-03785-02, 800-03785-03, 800-03785-04, 800-03785-05, 800-03785-06, 800-03785-07

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.

Determining Your NSP Part Number and Hardware Version

To determine the part number and hardware version of the NSP, use one of the following methods with information from [Table 5](#):

- If you are holding the board, look at the 800- part number label on the back of the NSP.
- If you can only view the faceplate of the NSP, look at the CLEI code label.
- Enter the **show hardware EXEC** command to display the NSP-PC and NSP-SC part numbers and hardware versions.

The following example displays the **show hardware** command output for an NSP:

```
Switch# show hardware

6400 named Switch, Date:17:51:21 UTC Thu Mar 9 2000
Feature Card's FPGA Download Version:0

Slot  Ctrlr-Type  Part No.  Rev  Ser No  Mfg Date  RMA No.  Hw Vrs  Tst  EEP
-----
1/0   NRP           73-3082-08 F0  17827878 Feb 02 00 00-00-00  4.255  0  2
2/0   NRP           73-3082-08 F0  17828272 Feb 02 00 00-00-00  4.255  0  2
3/0   NRP           73-3082-08 F0  17800617 Feb 16 00 00-00-00  4.255  0  2
4/0   NRP           73-3082-08 F0  17801802 Feb 22 00 00-00-00  4.255  0  2
5/0   NRP           73-3082-08 F0  17828075 Feb 06 00 00-00-00  4.255  0  2
7/0   NRP           73-3082-08 F0  17800637 Feb 16 00 00-00-00  4.255  0  2
8/0   622SM NLC      73-3868-02 A0  14327690 Oct 15 99 00-00-00  1.0    0  2
→ 0B/FC NSP-PC    73-2996-06 A0  15794042 Mar 05 00 00-00-00  1.1  0  2
0B/PC FC-PFQ     73-2281-04 B0  17803407 Mar 05 00 00-00-00  4.1    0  2
→ 0B/PC NSP-SC    73-2997-06 A0  17826384 Mar 05 00 00-00-00  1.0  0  2

Primary NSP:Slot 0B

DS1201 Backplane EEPROM:
Model Ver.  Serial  MAC-Address  MAC-Size  RMA  RMA-Number  MFG-Date
-----
C6400  2  17900239 000142C04900  128  0  0  Mar 04 2000

Switch#
```

**Note**

If your **show hardware** output shows the NSP-PC Part No. as 73-2996-03 and the NSP-SC Part No. as 73-2997-02, you have an NSP on which the part numbers were incorrectly programmed. Use the CLEI code to determine your NSP part number. If you cannot physically see the NSP, assume you have P/N 800-03785-03.

Table 5 NSP Part Numbers and Hardware Versions

CLEI Code	800- Part Number	NSP-PC		NSP-SC	
		Part No.	Hw Vrs	Part No.	Hw Vrs
BAC7R2HCAA	800-03785-08	73-2996-06	any	73-2997-08	any
BAC5DD7DAA	800-03785-07	73-2996-06	any	73-2997-07	any
BAC5DDVDAA	800-03785-06	73-2996-06	any	73-2997-06	any
BAC5DDVDAA	800-03785-05	73-2996-05	any	73-2997-05	any
BAC5DD0DAB	800-03785-04	73-2996-05	any	73-2997-04	any
BAC5DD0DAA	800-03785-03 (Deviation D99-3628) (Deviation D99-3178)	73-2996-04	1.1 (Dev. D99-3628 put Hw Vrs to 1.1)	73-2997-03	any
	800-03785-03 (Deviation D99-3628)	73-2996-04	1.1 (Dev. D99-3628 put Hw Vrs to 1.1)	73-2997-03	any
	800-03785-03 (Deviation D99-3178)	73-2996-04	any	73-2997-03	any
	800-03785-03	73-2996-04	any	73-2997-03	any

**Note**

Deviation labels might not be visible. If you cannot verify that your NSP has a particular deviation, assume it does not.

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 20](#)
- [Platform-Specific Documents, page 20](#)
- [Feature Modules, page 22](#)

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: Cross-Platform Release Notes

On the Documentation CD-ROM at:

Cisco IOS Software Configuration: Cisco IOS Release 12.1: Release Notes: Cross-Platform 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 6](#) 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 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"> 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 DB1 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 DB

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 DB

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 7 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 7 Cisco IOS Software 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
<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> 	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> 	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces

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

Books	Major Topics
<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
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	<ul style="list-style-type: none"> 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> 	<ul style="list-style-type: none"> 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

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

Books	Major Topics
<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 19](#)

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