



Text Part Number: 78-5281-09 Rev. -B0

Release Notes for Cisco 3600 Series Routers for Cisco IOS Release 11.3 NA

August 9, 1999

These release notes describe new features and significant software components for Cisco 3600 series routers that support Cisco IOS Release 11.3 NA, up to and including Release 11.3(11)NA, which is based on Cisco IOS Release 11.3. These release notes are updated as needed to accommodate new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes.

For a list of the software caveats that apply to Release 11.3 NA, refer to the “Caveats” section on page 12.

Use these release notes with the *Release Notes for Cisco 3600 Series for Cisco IOS Release 11.3 T* located on (CCO) and the Documentation CD-ROM.

Contents

These release notes discuss the following topics:

- Introduction, page 2
- System Requirements, page 2
- New and Changed Information, page 6
- Limitations and Restrictions, page 8
- Important Notes, page 9
- Caveats, page 12
- Related Documentation, page 17
- Service and Support, page 22
- Cisco Connection Online, page 23
- Documentation CD-ROM, page 23

Corporate Headquarters

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

Copyright © 1999
Cisco Systems, Inc.
All rights reserved.

Introduction

The Cisco 3600 series includes the Cisco 3620 and Cisco 3640 routers. As modular solutions, the Cisco 3620 and Cisco 3640 enable corporations to increase dial-up density and take advantage of current and emerging Cisco WAN technologies and networking capabilities. The Cisco 3600 series routers are fully supported by Cisco IOS software, which includes dial-up connectivity, LAN-to-LAN routing, data and access security, WAN optimization, and multimedia features.

System Requirements

This section describes the system requirements for Release 11.3(11)NA.

- Memory Requirements, page 2
- Hardware Supported, page 2
- Determining the Version of Your Software Release, page 4
- Upgrading to a New Software Release, page 4
- Feature Set List, page 5

Memory Requirements

Table 1 Release 11.3 NA Memory Requirements for the Cisco 3600 Series

Platform	Feature Set	Image Name	Minimum Required Code Memory	Required Main Memory	Runs from
Cisco 3620	IP/H323	c3620-ix-mz	4 MB Flash	32 MB DRAM	RAM
Cisco 3640	IP/H323	c3640-ix-mz	4 MB Flash	32 MB DRAM	RAM

Note The images in this release do not include encryption.

Hardware Supported

Cisco IOS Release 11.3(11)NA supports the Cisco 3600 series routers:

- Cisco 3620
- Cisco 3640

Table 2 lists the interfaces supported by the Cisco 3600 series.

Table 2 Supported Interfaces for the Cisco 3600 Series

Interface, Network Module, or Data Rate	Platforms Supported	
Dial Access Network Modules	16- and 32-port Asynchronous network module	All Cisco 3600 series platforms
	6- to 30-port Integrated Digital Modems network module	All Cisco 3600 series platforms
	8- or 16-port Integrated Analog network module	All Cisco 3600 series platforms

Table 2 Supported Interfaces for the Cisco 3600 Series (continued)

Interface, Network Module, or Data Rate	Platforms Supported
LAN Interfaces	1- and 4-port Ethernet (AUI and 10BaseT)
	4/16 Mbps Token Ring
	Fast Ethernet (100BaseTX and 100BaseFX)
Mixed Media Network Modules	Single port 10/100BaseTX with 1-port Channelized/PRI E1 balanced mode
	Single port 10/100BaseTX with 1-port Channelized/PRI E1 unbalanced mode
	Single port 10/100BaseTX with 1-port Channelized/PRI T1
	Single port 10/100BaseTX with 1-port Channelized/PRI T1 with CSU
	Single port 10/100BaseTX with 2-port Channelized/PRI E1 balanced mode
	Single port 10/100BaseTX with 2-port Channelized/PRI E1 unbalanced mode
	Single port 10/100BaseTX with 2-port Channelized/PRI T1
	Single port 10/100BaseTX with 2-port Channelized/PRI T1 with CSU
Voice/Fax Interfaces and Network Modules¹	1- and 2-port Voice/Fax network module
	2-port E&M Voice interface card
	2-port FXO Voice interface card
	2-port FXS Voice interface card
WAN Data Rates	48/56/64 kbps
	1.544/2.048 Mbps
	Up to 8 Mbps on 4-port Serial network module
	52 Mbps max using High Speed Serial Interface (HSSI) network module

Table 2 Supported Interfaces for the Cisco 3600 Series (continued)

Interface, Network Module, or Data Rate	Platforms Supported
WAN Interfaces and Network Modules²	1- and 2-port Channelized T1 and E1 network module
	1-port ATM-25 network modules for the Cisco 3600 series
	1-port BRI with NT or S/T WAN interface card
	1-Port High Speed Serial Interface (HSSI) network module
	4- and 8-port BRI network module with NT1
	4- and 8-port BRI network module with S/T interface
	4- and 8-port Synchronous/Asynchronous
	4-port Serial
	56/64 kbps DSU/CSU
	T1 WAN interface card for Cisco 3600, Cisco 2600, and Cisco 1600 series
	T1 with Integrated DSU/CSU for the Cisco 3600, Cisco 2600, and Cisco 1600 series

1 The Voice/Fax network modules require Cisco IOS Plus feature sets.

2 The ATM-25 network modules require Cisco IOS Plus feature sets.

Determining the Version of Your Software Release

To determine the version of Cisco IOS software currently running on the Cisco 3600 series router, log in to the Cisco 3600 series router and enter the **show version EXEC** command.

```
router>show version
Cisco Internetwork Operating System Software
IOS (tm) 3600 Software (C3620-IX-MZ), Version 11.3(11)NA, SHARED PLATFORM,
```

Upgrading to a New Software Release

For information about upgrading to a new software release, see the *Cisco IOS Software Release 11.3 Upgrade Paths and Packaging Simplification* product bulletin located on CCO at:

Service & Support: Product Bulletins: Software

Under **Cisco IOS 11.3**, click on **Cisco IOS Software Release 11.3 Upgrade Paths (#703: 12/97)**

The *Cisco IOS Software Release Upgrade Paths and Packaging Simplification* product bulletin does not contain information specific to Cisco IOS Release 11.3 NA, but provides general upgrade information that may apply to Cisco IOS Release 11.3 NA.

Feature Set List

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

This section lists Cisco IOS software features available in Cisco IOS Release 11.3(11)NA.

IP Routing

- Easy IP, Phase 1
- H.323 Voice over IP Gatekeeper
- Hot Standby Router Protocol (HSRP) Support
- E.164 Address Support
- Technology Prefixes
- IP Enhanced IGRP Route Authentication
- TCP Enhancements, including:
 - TCP Selective Acknowledgment
 - TCP Timestamp

Management

- Cisco IOS Internationalization
- Entity MIB, Phase 1
- SNMPv2C
- Virtual Profiles

Multimedia

- IP Multicast Load Splitting across Equal-Cost Paths
- IP Multicast over Token Ring LANs
- PIM Version 2
- Stub IP Multicast Routing

Quality of Service

- RTP Header Compression

Security

- Double Authentication
- HTTP Security
- Per-User Configuration
- Reflexive Access Lists
- Vendor-Proprietary RADIUS Attributes

New and Changed Information

Switching

- Fast-Switched Policy Routing

WAN Optimization

- PAD Subaddressing

WAN Services

- Bandwidth Allocation Control Protocol
- Dialer Watch
- Enhanced Local Management Interface (ELMI)
- Frame Relay Enhancements
- Frame Relay MIB Extensions
- Frame Relay Router ForeSight
- ISDN Caller ID Callback
- Leased-Line ISDN at 128 kbps
- MS Callback
- X.25 Enhancements
- X.25 Switching between PVCs and SVCs
- X.28 Emulation

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 3600 series routers in Cisco IOS Release 11.3 NA.

New Features in Releases 11.3(7)NA through 11.3(11)NA

There are no new features supported by the Cisco 3600 series routers in these releases.

New Software Features in Release 11.3(6)NA2

The following new software features are supported by the Cisco 3600 series routers in Cisco IOS Release 11.3(6)NA2.

H.323 Voice over IP Gatekeeper

The Gatekeeper can manage a zone and provide bandwidth management and address registration services to gateways that are present in the network. The Gatekeeper manages H.323 endpoints in a consistent manner, allowing them to register with a gatekeeper and to locate another gatekeeper. The Gatekeeper provides logic variables for proxies or gateways in a call path to provide connectivity with the public switched telephone network (PSTN), to improve Quality of Service (QoS), and to enforce security policies. Multiple gatekeepers may be configured to communicate with one another, either by integrating their addressing into Domain Naming System (DNS), or via Cisco IOS configuration options.

HSRP Support

Gatekeeper HSRP (Hot Standby Router Protocol) support consists of elements that affect both the gateway and gatekeeper functions in the router. The gateway periodically retries its registration when it detects a possible gatekeeper failure, in order to register itself with the backup gatekeeper. The backup gatekeeper normally operates in a passive mode in which it does not accept registrations, and becomes active only when it is notified by HSRP that it must become the primary gatekeeper.

E.164 Address Support

There are two types of addresses used in H.323 destination calls:

- H.323-ID (a character string)
- E.164 address (a string containing phone-keypad characters)

The Cisco IOS Release 11.3(2)NA software feature Multimedia Conference Manager dealt primarily with H.323-ID addressing in interzone calls. With the new prefix commands, the administrator can now also configure interzone routing when calls are made using E.164 addresses.

Technology Prefixes

Technology prefixes are designed to enable the use of E.164 address routing. E.164 is an International Telecommunications Union (ITU) specification for the ISDN international telephone numbering plan, which has traditionally only been used in telephone networks. These prefixes identify gateways that have specific capabilities within a given zone. They are handled specially in that the technology prefixes are ignored during the zone selection process and then examined for gateway selection within the zone.

New Features in Releases 11.3(4)NA through 11.3(6)NA

There were no new features supported by the Cisco 3600 series routers in these releases.

New Features in Release 11.3(3)NA

Cisco IOS Release 11.3(3)NA was not released.

New Software Features in Release 11.3(2)NA

The following new software features are supported by the Cisco 3600 series routers in Release 11.3(2)NA. The special Cisco IOS Release 11.3(2)NA image for Cisco 3600 series routers was *not* designed to perform as standard Cisco 3600 series router Cisco IOS software.

Multimedia Conference Manager

The Multimedia Conference Manager feature for Cisco 3600 series routers for Cisco IOS Release 11.3(2)NA is offered in the IP Standard Feature Set described as follows.

Cisco Multimedia Conference Manager provides network administrators with a mechanism to support ITU-T H.323 applications without impacting the mission-critical applications that are running on today's networks. Multimedia Conference Manager also provides the mechanism to implement security for H.323 communications. The image has specialized features designed specifically for the Multimedia Conference Manager feature (gatekeeper and proxy conforming to ITU-T H.323).

H.323 Multimedia Conference Manager, implemented on Cisco IOS software, provides the network administrator with the ability to do the following:

- Identify H.323 traffic and apply appropriate policies
- Limit the H.323 traffic on the LAN/WAN
- Provide user accounting with records based on the service utilization
- Inject Quality of Service (QoS) for the H.323 traffic generated by applications such as VoIP, data conferencing, and videoconferencing

H.323 Proxy

The H.323 gatekeeper is an infrastructure component defined by the ITU H.323 standard. It provides call routing functionality for H.323 endpoints, provides simple bandwidth management for H.323, and adds authentication, authorization, and accounting functionality for H.323 calls.

The H.323 proxy is included in the Multimedia Conference Manager feature. The H.323 proxy is a boundary device that terminates all H.323 calls from the local LAN/Zone and can establish sessions with H.323 endpoints that are in a different LAN/Zone. In doing so, the proxy provides the administrator the ability to set and enforce Quality of Service (QoS) policy on WAN segments, and provides a method to tag H.323 traffic for tunneling through firewalls.

Limitations and Restrictions

The limitations described in this section apply to this special release.

SNMP Support for Multimedia Conference Manager

The H.323 gatekeeper and proxy features in this release currently do not support SNMP-based management. All standard features in this release do include support for SNMP-based management.

One Gateway per Zone

The current Cisco gatekeeper supports only one gateway per zone. More than one gateway is allowed to register per zone; however calls are not forwarded to that gateway.

One Proxy per Zone

The current Cisco gatekeeper supports only one H.323 proxy per zone. More than one proxy is allowed to register per zone; however, calls are not forwarded to that proxy.

No Voice Gateways

The current Cisco gatekeeper supports only H.320 gateways. Voice gateways are not supported. Voice gateways are allowed to register; however, calls are not forwarded to them.

Only One Local-Zone Declaration Supported

The current Cisco gatekeeper supports only one local-zone declaration. Declarations of more than one local zone in the Cisco gatekeeper are flagged as errors.

Important Notes

The following section applies to Cisco IOS Release 11.3 NA up to and including Cisco IOS Release 11.3(11)NA.



Caution In certain countries, use of these products or provision of voice telephony over the Internet may be prohibited and/or subject to laws, regulations or licenses, including requirements applicable to the use of the products under telecommunications and other laws and regulations; customers must comply with all such applicable laws in the country(ies) where they intend to use the products.

Cisco IOS Release 11.3, 11.3 NA and 11.3 T End of Sales and End of Engineering

End of Engineering (EOE) means there are no more regularly scheduled maintenance releases. The last maintenance release scheduled on the EOE date is only available through CCO and Field Service Operations—not through manufacturing.

- Cisco IOS Releases 11.3, 11.3 NA, and 11.3 T are scheduled to reach End of Sales (EOS) status with maintenance Releases 11.3(10), 11.3(11)NA, and 11.3(10)T.
- Releases 11.3, 11.3 NA, and 11.3 T are scheduled to reach EOE with Releases 11.3(11), 11.3(11)NA, and 11.3(11)T.

EOS and EOE releases are subject to change. For the most up-to-date information on the status of EOS or EOE, refer to the *End of Sales and End of Engineering for Cisco IOS Software Releases* product bulletins located on CCO.

Ongoing support for functionality in Releases 11.3, 11.3 NA, and 11.3 T is available in Cisco IOS Release 12.0(3)T and later maintenance releases of Cisco IOS Release 12.0.

On CCO, click on this path:

Service & Support: Product Bulletins: Software

Under **Cisco IOS 11.3**, click on **End of Sales and End of Engineering for Cisco IOS Software Releases 11.3 and 11.3 T (#847: 12/98)** or **Cisco IOS Software 11.3 NA EOS and EOE (#849:12/98)**

Image Deferral, Cisco IOS Release 11.3(8)T

Cisco IOS Release 11.3(8)T was deferred to Release 11.3(8)T1 on all software images to incorporate corrections to the following caveats:

- CSCdk86294—The D channel is always in the shutdown state when non-facility associated signalling is configured.
- CSCdk80809—Enhanced Interior Gateway Routing Protocol (EIGRP) has difficulty converging on certain routes.

For more information on these caveats, refer to Bug Navigator II. Bug Navigator II is available at <http://www.cisco.com/support/bugtools>. On CCO, click this path:

Service & Support: Online Technical Support: Software Bug Toolkit: Bug Navigator II

Use as a Dedicated Router Only

A Cisco 3600 series router using the Multimedia Conference Manager feature is designed to be used as a dedicated router. Do not use the Multimedia Conference Manager on a regular router. The Multimedia Conference Manager can take up a significant amount of CPU process time when a H.323 call is being established through the proxy. The impact of the call establishment on the routing performance is not currently fully determined; however, it is advisable that a Cisco 3600 series router with Multimedia Conference Manager *not* be used as a regular router.

Enabling the Release Special Image

The special Cisco IOS Release 11.3(2)NA image for Cisco 3600 series routers was *not* designed to perform as standard Cisco 3600 series router Cisco IOS software. The image has specialized features designed specifically for the Multimedia Conference Manager feature (gatekeeper and proxy conforming to H.323). Be sure to enable these features on routers running this release. Multimedia Conference Manager is briefly described in the previous section. For more information, see the Multimedia Conference Manager feature online documentation. See the “Related Documentation” section on page 17.

ATM Multipoint Signaling

Prior to Cisco IOS Release 11.1(13) and 11.2(8), the **atm multipoint-signaling** command was used on the main interface and affected all subinterfaces. For Release 11.1(13), 11.2(8), and later releases (including Release 11.3), explicit configuration on each subinterface is required to obtain the same functionality. Refer to caveat CSCdj20944, which is described as follows:

The **atm multipoint-signaling** interface command is currently only available on the main ATM interface. The effect is that signaling behavior (point-to-point or point-to-multipoint) for all clients on all subinterfaces is determined by the command on the main interface.

Clients on different subinterfaces can have different behavior. Specifically, 1577 requires point-to-point, and PIM allows point-to-multipoint. The command should be on a per subinterface basis.

Enable the **atm multipoint-signaling** command on all subinterfaces that require it. Previously, you only needed to enable the command on the main interface.

Enabling IPX Routing

Whenever IPX routing is enabled, the Token Ring interface resets.

Forwarding of Locally Sourced AppleTalk Packets

Cisco’s implementation of AppleTalk does not forward packets with local-source and destination network addresses. This behavior does not conform to the definition of AppleTalk in Apple Computer’s *Inside AppleTalk* publication. However, this behavior is designed to prevent any possible corruption of the AppleTalk Address Resolution Protocol (AARP) table in any AppleTalk node that collects MAC-addresses.

Missing Source-Route Bridging Commands

Due to a production problem, many source-route bridging commands were omitted from the printed version of the *Cisco IOS Software Command Summary (78-4746-XX)*. For documentation of all source-route bridging commands, refer to the *Bridging and IBM Networking Command Reference (78-4743-XX)*. You can also obtain the most current documentation on CCO or on the Documentation CD-ROM.

New TACACS+ Attribute-Value Pair

A new authorization feature that allows you to separately configure and authorize Multilink PPP was added in Cisco IOS Release 11.3(1). This feature can cause MLP authorization to fail in TACACS+ servers that do not include the relevant authorization permissions in the configuration.

For TACACS+, add the following attribute-value (AV) pair for all users who are allowed to negotiate Multilink PPP:

```
service = ppp protocol = multilink {
```

Using LAN Emulation

Note the following information regarding the LAN Emulation (LANE) feature in Cisco IOS Release 11.3:

- LANE is available for use with Cisco 4500 and Cisco 4700 series routers, and Cisco 7000 and Cisco 7500 series routers connected to either an LS100 or LS1010 switch. LANE requires at least Version 3.1(2) of the LS100 software, which requires a CPU upgrade if you are currently running software earlier than Version 2.5.
- Do not use the LS2020 for LANE because it does not support UNI 3.0 and point-to-multipoint SVCs.
- Routing of IP, IPX, AppleTalk, DECnet, VINES, and XNS is supported.
- Hot Standby Router Protocol (HSRP) is supported.
- LANE does not support Connectionless Network Service (CLNS) or LANE over Permanent Virtual Circuits (PVCs).
- Do not route AppleTalk Phase 1 to AppleTalk Phase 2 by using LANE.

Deprecated MIBs

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. OLD-CISCO-* MIBs are currently being migrated into more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown in the following table.

Table 3 **Deprecated and Replacement MIBs**

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	In Development
OLD-CISCO-DECNET-MIB	

Table 3 **Deprecated and Replacement MIBs**

Deprecated MIB	Replacement
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBS)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	

Caveats

Caveats describe unexpected behavior or defects in Cisco IOS software releases. This section only contains open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Release 11.3 and Release 11.3 T are also in Release 11.3(11)NA.

For information on caveats in Cisco IOS Release 11.3, refer to the “Important Notes and Caveats for Release 11.3” section in the cross-platform *Release Notes for Cisco IOS Release 11.3* document, which is located on CCO and the Documentation CD-ROM. These release notes list severity 1 and 2 caveats affecting all maintenance releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

For information on caveats in Cisco IOS Release 11.3 T, refer to the *Caveats for Cisco IOS Release 11.3 T* document, which is 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. From CCO, log in and click on this path: **Service & Support: Online Technical Support: Software Bug Toolkit**. You can also find Bug Navigator II at <http://www.cisco.com/support/bugtools>.

Open Caveats—Release 11.3(1)NA through 11.3(11)NA

This section describes possibly unexpected behavior by Release 11.3(11)NA. Unless otherwise noted, these caveats apply to all 11.3 releases up to and including 11.3(11)NA.

Miscellaneous

- CSCdm47012

The latest versions of Smart Modular and Sharp Flash cards used to store Diagnostics and IOS SW images can report unrecoverable write errors.

Affected Flash cards use a new Sharp (LH28F016SCT) chip set. The original Smart Modular and Intel Flash cards are not affected.

Affected platforms are 7200 and all derivatives, 7500, GSR, and maybe others.

There is no workaround. If the problem occurs, try to reformat the Flash, store less images, or try storing images in a different order. This may help under some circumstances.

- CSCdm68266

When running 11.3(10)NA image, ingress gw can display wrong cause code.

- CSCdm68546

This fixes CM status display in CMTS when the modem goes offline with BPI turned on and key expiration.

Resolved Caveats—Release 11.3(11)NA

All the caveats listed in this section are resolved in Release 11.3(11)NA. This section describes only severity 1 and 2 caveats.

Basic System Services

- CSCdk80230

Certain Internetwork Status Monitor (ISM) NetView users can issue non-enable mode commands without router authentication. Users accessing the router through NetView must be authenticated through NetView's security methods, which can include RACF and SAF. Mainframe users can be restricted from issuing any router commands by the restriction of the RUNCMD within NetView. Users issuing enable mode commands must be authorized to issue this level of command by ISM, and must possess the ENABLE mode password. If the router is controlled by TACACS+, the ISM user must have a TACACS+ User ID and Password to issue enable level commands.

show user : command has been modified : the user field is filled up by the host name.

Two options have been added to the following commands : **sna host** and **dspu host**.

The options are: **no-enable** and **high-security**.

Configure these options with focalpoint.

no-enable : when this is set, it does not allow enable command from the host

high-security : when this is set, it allows the following commands in USER mode. (PRIVILEGE mode is not affected by this option.) You must enter all these commands in full or else the command will not be allowed (that is, sh versi is not allowed for **show version**)

DECnet

- CSCdk23805
When decnet accounting is implemented, it's possible for the router to crash depending on the amount of connections.
- CSCdm28939
When you are configuring Decnet on a router, you can specify an Address Translation Gateway (ATG) network number in the range 0 to 3. If the *ATG-network-number* is specified incorrectly while configuring an interface, the router will reload.
If the *ATG-network-number* is not required the problem will not occur.
If the *ATG-network-number* is required, then a workaround is to ensure that the *ATG-network-number* specified when enabling an interface matches the *ATG-network-number* specified when decnet routing is enabled globally; for example:
decnet 1 routing 2.3 interface ethernet 0/0 decnet 1 cost 5

EXEC and Configuration Parser

- CSCdm39355
If the length of the entire command after completion exceeds PARSEBUF, then the router crashes
Fix: Don't allow the "command completion" if it exceeds PARSEBUF

IBM Connectivity

- CSCdm39124
Console message flooding may occur when an XID3 loop occurs with APPN in the router. The following messages are repeated for each iteration of the loop:

```
%APPN-3-logcsCS_XXXXIP11_LOGMSG_01: CS - Sending Alert to MS, sense_code = 83E0001,
proc_name = XXXXIP32, port_name = HMAC04, ls_name = @LS00289
%APPN-3-logcsCS_XXXXIP11_LOGMSG_03: CS - Associated outbound XID data in alert (length
>= 29): %APPN-3-Error:
32730770000000000000F7C1000000008000010B51000500000000007000E11F4C4C5C2E5D4E4F0F04BD5D5C
3C9D7F0F110380037110C0804F1F2F0F0F0F00908F0F0F0F0F0F01406C3C9E2C3D640C1D7D7D540D5D561
C4D3E4D90F0FC3C9E2C3D640C1D7D7D540D5D522070000000083E0001
%APPN-3-logcsCS_XXXXIP11_LOGMSG_05: CS - Associated inbound XID data in alert (length
>= 29): %APPN-3-Error:
326705D56F010000B008100000000000010B410005B800000000070010370023110C0804F0F3F0F0F0F0
F06D4E240E2D5C140E2C5D9E5C5D90908F0F0F0F0F0F0131103100010F0F0F0F0F0F0F0F0F0F0F0F00E
0FF4C4C5C2E5D4E4F0F04BC3E3F5F6C6
```


Avoid console logging.
- CSCdm49573
The router crashes with bus error when executing a **show dlsw circuit** command if there is a circuit with a local rif of 18 bytes.
This is a regression introduced by CSCdk83294.
- CSCdm50361
DLSw Lite peers leak CLS connect request buffers. If possible, try using a different peer type.
This patch frees an outstanding connect request if additional requests are received while the first request is still pending.

Interfaces and Bridging

- CSCdk10376

SYMPTOM: Crash in frf9_preComp()

This condition most frequently occurs during times when router traffic is heavy, which causes memory usage to increase and a possible low-memory condition to occur.

WORKAROUND: Disable compression or use a different type.

Since this problem is aggravated by a low-memory condition, tuning the memory can prevent this condition from occurring, but there are no guarantees.

- CSCdm41644

This is caused by an over-write issue in bss area with FDDI modules equipped which has potential to cause serious problem such as crash in 12.0T.

- CSCdm46735

A PA-4R-DTR port may reset under the following circumstances:

- 1) A high rate of traffic is traversing the port (200 pps or better) .
- 2) The PA-4R-DTR port is the active monitor of the physical ring.
- 3) An event on the ring forces the active monitor to purge the ring.

When this problem occurs, the PA-4R-DTR port resets, and the ring experiences a beacon.

Workaround: Make sure the DTR port is not the active monitor on the ring. This can be done by ensuring that the mac-address of the DTR card is not the highest mac-address on the physical ring.

IP Routing Protocols

- CSCdm20483

IP access lists fail to block pings on the interfaces configured for policy routing with IP route-cache policy.

- CSCdm28898

ARP to a router fails on the serial interface when bridging is enabled and after the router is reloaded.

```
----eth---2500---serial---2500---eth---
```

Router : 2500 IOS : 112.(17), 12.0(3.7)

Workaround: Remove IP address on serial and enter again.

- CSCdm44957

Some IP fragments may be incorrectly filtered out by access lists.

- CSCdm53317

DNS replies passing from "inside" to "outside" through NAT are not NAT translated correctly in many cases. There is no work around.

- CSCdm30090
When the router is operating as an X.25 switch and forwards an X.25 call containing certain facilities not interpreted by the router, the facility values can be corrupted. The problem most likely occurs when the call cannot be forwarded immediately (i.e., when using X25-over-TCP) with heavy traffic; the affected facilities include any local facilities and the Charging Information facility.
- CSCdm33448
A router performing X.25 switching may reload when clearing many calls simultaneously during heavy traffic.
- CSCdm36123
Customer repeatedly crashes (segV) when dialer rotor best is configured and 'deb dialer' is started once the traffic triggers a call.
- CSCdm37653
Reliable PPP can cause an intermittent crash when used with WFQ. Workaround is to disable Reliable PPP or WFQ.
- CSCdm38291
The router configured for dialer watch never dials back when backup interface times out if Watched route on dialer watch is not installed in routing table.

Related Documentation

The following sections describe the documentation available for the Cisco 3600 series routers. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, and feature modules, which are available online on CCO and the Documentation CD-ROM.

Use these release notes with the documents listed in the following sections:

- Release-Specific Documents, page 17
- Platform-Specific Documents, page 18
- Feature Modules, page 19
- Cisco IOS Software Documentation Set, page 19

Release-Specific Documents

The following documents are specific to Release 11.3. They are located on CCO and the Documentation CD-ROM:

- *Release Notes for Cisco IOS Release 11.3*

To reach the cross-platform *Release Notes for Cisco IOS Release 11.3* on CCO:

Service & Support: Technical Documents: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3

To reach the cross-platform *Release Notes for Cisco IOS Release 11.3* on the Documentation CD-ROM, follow this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Release Notes for Cisco IOS Release 11.3

- Product bulletins, field notices, and other release-specific documents

To reach these documents from CCO, click on this path:

Service & Support: Technical Documents

- Caveats

As a supplement to the caveats listed in the “Caveats” section on page 12 in these release notes, see the *Caveats for Cisco IOS Release 11.3 T* document, which contains caveats applicable to all platforms for all maintenance releases of Release 11.3 NA.

On CCO at:

Service & Support: Technical Documents: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Product Specific Release Notes for Cisco IOS Release 11.3: Caveats for Cisco IOS Release 11.3 T

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Product Specific Release Notes for Cisco IOS Release 11.3: Caveats for Cisco IOS Release 11.3 T

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. From CCO, log in and click on this path: **Service & Support: Online Technical Support: Software Bug Toolkit**. You can also find Bug Navigator II at <http://www.cisco.com/support/bugtools>.

Platform-Specific Documents

The documents listed below are available for the Cisco 3600 series routers. These documents are also available online at Cisco Connection Online (CCO) and on the Documentation CD-ROM.

- *Cisco 3620 Router Installation and Configuration Guide*
- *Cisco 3640 Router Installation and Configuration Guide*
- *Network Module Hardware Installation Guide*
- *Update to Network Module Hardware Installation Guide and Software Configuration Guide*
- *WAN Interface Cards Hardware Installation Guide*
- *Update to WAN Interface Cards Hardware Installation Guide*
- *Cisco 3600 Series Configuration Notes*
- *Regulatory Compliance and Safety Information for the Cisco 3600 Series*

On CCO at:

Service & Support: Technical Documents: Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 3600 Series

On the Documentation CD-ROM at:

Cisco Product Documentation: Access Servers and Access Routers: Modular Access Routers: Cisco 3600 Series

Feature Modules

Feature modules describe new features supported by Release 11.3 T and are an update to the Cisco IOS documentation set. Feature modules consist of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the features modules are only available online. The feature module information is included in the next printing of the Cisco IOS documentation set.

On CCO at:

Service & Support: Technical Documents: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS 11.3T New Features

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS 11.3T New Features

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. These documents 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: configuration guides and command references.

On CCO at:

Service & Support: Technical Documents: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS 11.3 Configuration Guides, Command References: Configuration Guide Master Index or Command Reference Master Index

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3: Cisco IOS 11.3 Configuration Guides, Command References: Configuration Guide Master Index or Command Reference Master Index

To reach documentation related to an index entry, click on the page number following the entry.

Release 11.3 Documentation Set

Table 4 details the contents of the Cisco IOS Release 11.3 software documentation set. The document set is available in electronic form, and also in printed form upon request.

Note You can find the most current Cisco IOS documentation on the latest Documentation CD-ROM and on the Web. These electronic documents may contain updates and modifications made after the paper documents were printed.

You can reach the Cisco IOS documentation set on CCO at:

Service & Support: Technical Documents: Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3

You can reach the Cisco IOS documentation set on the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 11.3

Table 4 Cisco IOS Release 11.3 Software Documentation Set

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Configuration Fundamentals Configuration Guide</i> • <i>Configuration Fundamentals Command Reference</i> 	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management Interface Configuration System Management
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 1</i> • <i>Network Protocols Command Reference, Part 1</i> 	IP Addressing IP Services IP Routing Protocols
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 2</i> • <i>Network Protocols Command Reference, Part 2</i> 	AppleTalk Novell IPX
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 3</i> • <i>Network Protocols Command Reference, Part 3</i> 	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Wide-Area Networking Configuration Guide</i> • <i>Wide-Area Networking Command Reference</i> 	ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> • <i>Security Configuration Guide</i> • <i>Security Command Reference</i> 	AAA Security Services Security Server Protocols Traffic Filtering Network Data Encryption Other Security Feature

Table 4 Cisco IOS Release 11.3 Software Documentation Set (continued)

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Dial Solutions Configuration Guide</i> • <i>Dial Solutions Command Reference</i> 	Business Applications and Scenarios Dial-In Terminal Service and Remote Node Configuration Dial Authentication Dial-on-Demand Routing Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Dialup Networks Other Network Traffic on ISDN Channels Dial-Related Addressing Services
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Switching Paths NetFlow Switching Overview of Routing between Virtual LANs Routing between VLANs with ISL Encapsulation Routing between VLANs with IEEE 802.10 Encapsulation LAN Emulation (LANE) Overview LAN Emulation
<ul style="list-style-type: none"> • <i>Bridging and IBM Networking Configuration Guide</i> • <i>Bridging and IBM Networking Command Reference</i> 	Bridging and IBM Networking Overview Bridging IBM Networking
<ul style="list-style-type: none"> • <i>Cisco IOS Software Command Summary</i> • <i>Dial Solutions Quick Configuration Guide</i> • <i>System Error Messages</i> • <i>Debug Command Reference</i> 	

Note Due to a production problem, many **source-route bridging** commands were omitted from the printed version of the *Cisco IOS Software Command Summary* (78-4746-01). For complete documentation of all **source-route bridging** commands refer to the *Bridging and IBM Networking Command Reference* (78-4743-01). You can also obtain the most current documentation on Cisco Connection Online (CCO) or on the Documentation CD-ROM.

Service and Support

For service and support for a product purchased from a reseller, contact the reseller. Resellers offer a wide variety of Cisco service and support programs, which are described in the section “Service and Support” in the information packet that shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems’ primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

Software Configuration Tips on the Cisco Technical Assistance Center Home Page

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

http://www.cisco.com/kobayashi/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your Web browser to CCO and click on this path: **Products & Technologies: Products: 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—Designed to notify you of any critical issues regarding Cisco products. These notices include problem descriptions, safety or security issues, and hardware defects.
- Hardware—Technical Tips related to specific hardware platforms.
- Hot Tips—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—Tips on using and deploying Cisco IOS software features and services.
- Sample Configurations—Actual configuration examples that are complete with topology and annotations.
- Software Products—MultiNet & Cisco Suite 100, Network Management, Cisco IOS Software Bulletins, and CiscoPro Configurations.
- Special Collections—Other Helpful Documents, including Case Studies, References & Request for Comments (RFCs), and Security Advisories.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

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

This document is to be used in conjunction with documents mentioned in the "Related Documentation" section on page 17.

Access Registrar, AccessPath, Any to Any, AtmDirector, CCDA, CCDE, CDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, CiscoLink, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Technologies logo, ConnectWay, ControlStream, Fast Step, FireRunner, GigaStack, IGX, JumpStart, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, Packet, PIX, Point and Click Internetworking, Policy Builder, Precept, RouteStream, Secure Script, ServiceWay, SlideCast, SMARTnet, StreamView, The Cell, TrafficDirector, TransPath, ViewRunner, VirtualStream, VisionWay, VlanDirector, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9907R)

Copyright © 1999, Cisco Systems, Inc.
All rights reserved.