



Text Part Number: 78-5862-07 Rev. E0

Caveats for Cisco IOS Release 11.3 T

June 16, 2004

This document lists severity 1 and 2 caveats for Cisco IOS Release 11.3 T, up to and including Cisco IOS Release 11.3(11b)T5. Caveats describe unexpected behavior or defects in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. This caveats document is revised for each maintenance release of Cisco IOS Release 11.3 T to document the latest caveats.

To improve this document, we would appreciate your comments. If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically at <http://www.cisco.com/feedback/> or contact caveats-doc@cisco.com. For more information, see the “Documentation CD-ROM” section on page 45.

How to Use This Document

This document describes open and resolved severity 1 and 2 caveats:

- The “Open Caveats—Release 11.3(11)T” section lists open caveats that apply to the current maintenance release, and might apply to previous maintenance releases.
- The “Resolved Caveats” sections list caveats that have been resolved in a particular maintenance release but were open in previous maintenance releases.

Within the sections, the caveats are sorted by technology in alphabetical order. For example, AppleTalk caveats are listed separately from, and before, IP caveats. The caveats are also sorted alphanumerically by caveat number.

If You Need More Information

The most up-to-date documentation can be found on the Web through Cisco Connection Online (CCO) and on the latest Documentation CD-ROM. These electronic documents might contain updates and modifications made after the paper documents were printed. For information on CCO, see the “Cisco Connection Online” section on page 44. For more information on the CD-ROM, see the “Documentation CD-ROM” section on page 45.

Corporate Headquarters

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

Copyright © 1999-2004
Cisco Systems, Inc.
All rights reserved.

For more information on caveats and features in Cisco IOS Release 11.3 T, see the following sources:

- *Internetworking Terms and Acronyms*—The *Internetworking Terms and Acronyms* document contains definitions of acronyms that are not defined in this caveats document.
- Bug Navigator II—If you have an account on Cisco Connection Online (CCO), you can use Bug Navigator II to find caveats of any severity for any release. Access Bug Navigator II at <http://www.cisco.com/support/bugtools>, or from CCO by logging on and selecting **Service & Support: Online Technical Support: Software Bug Toolkit: Bug Navigator II**.
- “Important Notes and Caveats for Release 11.3”—This section of the cross-platform release notes describes software caveats and important notes for Cisco IOS Release 11.3. All caveats in Cisco IOS Release 11.3 are also in Cisco IOS Release 11.3 T.
- *Release Notes for Cisco IOS Release 11.3 T*—These release notes describe new features and significant software components for Cisco IOS Release 11.3 T.
- *Release Notes for Cisco IOS Release 11.3*—These release notes describe new features and significant software components for Cisco IOS Release 11.3. All features in Cisco IOS Release 11.3 are also in Cisco IOS Release 11.3 T.
- Product-Specific Release Notes for Cisco IOS Release 11.3—These release notes describe new features and significant software components for Cisco IOS Release 11.3 T.
- What’s Hot for Cisco IOS Software Release 11.3—What’s Hot for Cisco IOS Software Release 11.3 provides information about caveats that are related to deferred software images for Cisco IOS Release 11.3 and Release 11.3 T. If you have an account on Cisco Connection Online (CCO), you can access What’s Hot for Cisco IOS Software Release 11.3 from CCO by logging on and clicking **Service & Support: Software Center: Cisco IOS Software: Cisco IOS 11.3: What’s Hot for Cisco IOS Software Release 11.3**.

Note Release notes are modified on an as-needed basis only. The maintenance release number and the revision date represent the last time the release notes were modified to include new or updated information. For example, release notes are modified whenever any of the following items change: software or hardware features, feature sets, memory requirements, software deferrals for the platform, microcode or modem code changes, announcements of important notes, or alterations to related documents.

The following table lists the most recent release notes when this caveats document was published:

Platform-Specific Release Notes	Cisco IOS Release	Revision Date
Cisco 1000 Series Routers	Release 11.3(11)T	August 2, 1999
Cisco 1600 Series Routers	Release 11.3(11)T	August 2, 1999
Cisco 2500 Series Routers	Release 11.3(11)T	August 2, 1999
Cisco 2600 Series Routers	Release 11.3(11)T	August 2, 1999
Cisco 3600 Series Routers	Release 11.3(11)T	August 2, 1999
Cisco 4000 Series Routers	Release 11.3(11)T	August 2, 1999
Cisco AS5100 and AS5200 Access Servers	Release 11.3(11)T	August 2, 1999
Cisco AS5300 Access Servers	Release 11.3(11)T	August 2, 1999

Cisco 7000 Family Routers	Release 11.3(11)T	August 2, 1999
Cisco UBR7200 Series Routers	Release 11.3(11)T	August 2, 1999
Release Notes for Catalyst 5000 Series RSM/VIP2 Cisco IOS 11.3T Software Releases	Release 11.3(11)T	August 2, 1999

Resolved Caveats—Release 11.3(11b)T5

Cisco IOS Release 11.3(11b)T5 is a rebuild release for Cisco IOS Release 11.3(11). The caveats in this section are resolved in Cisco IOS Release 11.3(11b)T5 but may be open in previous Cisco IOS releases.

- CSCdu53656

A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at <http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml>.

- CSCea28131

A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at <http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml>.

Resolved Caveats—Release 11.3(11b)T4

Cisco IOS Release 11.3(11b)T4 is a rebuild release for Cisco IOS Release 11.3(11). The caveats in this section are resolved in Cisco IOS Release 11.3(11b)T4 but may be open in previous Cisco IOS releases.

- CSCed27956

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

- CSCed38527

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

Resolved Caveats—Release 11.3(11b)T3

Cisco IOS Release 11.3(11b)T3 is a rebuild release for Cisco IOS Release 11.3(11). The caveats in this section are resolved in Cisco IOS Release 11.3(11b)T3 but may be open in previous Cisco IOS releases.

- CSCea02355

Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

Cisco has made software available, free of charge, to correct the problem.

This advisory is available at:

<http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml>

Resolved Caveats—Release 11.3(11b)T2

Cisco IOS Release 11.3(11b)T2 is a rebuild release for Cisco IOS Release 11.3(11). The caveats in this section are resolved in Cisco IOS Release 11.3(11b)T1 but may be open in previous Cisco IOS releases.

- CSCdw65903

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

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

Resolved Caveats—Release 11.3(11b)T1

Cisco IOS Release 11.3(11b)T1 is a rebuild release for Cisco IOS Release 11.3(11). The caveats in this section are resolved in Cisco IOS Release 11.3(11b)T1 but may be open in previous Cisco IOS releases.

- CSCdp11863

Cisco IOS software releases based on versions 11.x and 12.0 contain a defect that allows a limited number of SNMP objects to be viewed and modified without authorization using a undocumented ILMI community string. Some of the modifiable objects are confined to the MIB-II system group, such as “sysContact”, “sysLocation”, and “sysName”, that do not affect the device's normal operation but that may cause confusion if modified unexpectedly. The remaining objects are contained in the LAN-EMULATION-CLIENT and PNNI MIBs, and modification of those objects may affect ATM configuration. An affected device might be vulnerable to a denial-of-service attack if it is not protected against unauthorized use of the ILMI community string.

The vulnerability is only present in certain combinations of IOS releases on Cisco routers and switches. ILMI is a necessary component for ATM, and the vulnerability is present in every IOS release that contains the supporting software for ATM and ILMI without regard to the actual presence of an ATM interface or the physical ability of the device to support an ATM connection.

To remove this vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is documented in DDTS record CSCdp11863.

In lieu of a software upgrade, a workaround can be applied to certain IOS releases by disabling the ILMI community or “*ilmi” view and applying an access list to prevent unauthorized access to SNMP.

Any affected system, regardless of software release, may be protected by filtering SNMP traffic at a network perimeter or on individual devices.

This notice will be posted at

<http://www.cisco.com/warp/public/707/ios-snmplmi-vuln-pub.shtml>.

- 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.

[Part of the text was taken from rfc 1771.]

- CSCds04747

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

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

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

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

This notice will be posted at

<http://www.cisco.com/warp/public/707/ios-tcp-isn-random-pub.shtml>.

Open Caveats—Release 11.3(11)T

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

Basic System Services

- CSCdk51178

The disconnect-cause and disconnect-cause-ext attributes are missing in the Terminal Access Controller Access Control System Plus (TACACS+) network accounting stop record.

There is no known workaround.

- CSCdk75738

When Ascend compression is configured to Microsoft Point-to-Point Protocol (PPP) compression, Cisco RADIUS code misinterprets the Ascend compression as a stac compression.

There is no known workaround.

- CSCdk94141
When the terminal issues a printing command on a Cisco 2600 series router to the UNIX host, the router loses the first frame collections.
There is no known workaround.
- CSCdm48446
On a Cisco AS5200 series access server, AAA Accounting using RADIUS retransmits an accounting stop record with the delay-time equal to the radius-server timeout. This only happens on bonded ISDN calls that last for 2 minutes or longer.
There is no known workaround.

IBM Connectivity

- CSCdm11922
If you have a data-link switching (DLSw) direct encapsulation serial link WAN with an Ethernet LAN on one side and Token Ring LAN on the other, connections can only be established from the Token Ring side.
Workaround: Raise the maximum transmission unit (MTU) of the serial WAN to approximately 1800 bytes.
- CSCdm57726
A reload might occur when removing a serial tunnel from a Cisco 2600 series router.
There is no known workaround.

Interfaces and Bridging

- CSCdj88421
When the MAC address of an ATM interface is changed, the interface is reset and the switched virtual circuits on the interface are removed. Later, when the upper layer code tries to disconnect these virtual circuits, the requests are rejected. This causes the virtual circuit descriptors (VCDs) of these virtual circuit (VCs) to be in a “Delete Pending” state, and they cannot be used again.
Workaround: Use the **shutdown** command on the interface before changing the MAC address and then use the **no shutdown** command to enable the interface.
- CSCdj91477
When encapsulation is changed on a PRI interface, B-channel interfaces are set in the Up state. This causes the first call to the B channel to fail, but subsequent calls to that channel work after the first failure.
Workaround: When changing encapsulation on a PRI interface, you must first use the **shutdown** command on the interface before configuring the new encapsulation.
- CSCdk64927
A Cisco router might experience high (55–99%) CPU utilization.
Workaround: Turn off Frame Relay compression.

- CSCdm17766
ISDN Layer 2 will not initialize with High-Level Data Link Control (HDLC) and Stac compression combined.
Workaround: Run Cisco IOS Release 11.3(8.3)AA or disable Stac compression.
- CSCdm32737
When **stac compression** and **no fair-queuing** are configured on a channel-group interface and traffic increases, delays can occur on other channel groups. This can result in poor voice quality if VoIP is running over the other channel groups.
Workaround: Use PPP instead of HDLC.
- CSCdm47892
A Cisco 7500 series router running the rsp-jsv40-mz (Enterprise 40) software image on Cisco IOS Release 11.3 (9.2)T might experience a bus error.
There is no known workaround.

IP Routing Protocols

- CSCdm53724
A ping from a Cisco 7200 series router fails to reach to an IP address of a physical unit under the channel while using Cisco IOS Release 11.3(9)T with XCPA-26-8.
There is no known workaround.
- CSCdm65336
When an ethernet line is disconnected on a Cisco 2600 series router, the Switched Multimegabit Data Service (SMDS) link might fail.
There is no known workaround.

Miscellaneous

- CSCdk20218
Modem or asynchronous calls appear to overwrite the channel data that is already in use by an ISDN call (CISCO-POP-MIB).
There is no known workaround.
- CSCdk35262
Configuring Cisco IOS Release 11.3(4)T1 on a Cisco 2600 router and attempting to establish an IPSec tunnel to an Ascend router that is running beta IPSec code might cause the router to reload.
There is no known workaround.
- CSCdk53725
When the serial 0:23 interface is used as a backup interface, the “return to operational” status of the backed up interface might cause the T1 line to go down and put the switch (a Nortel DMS250) into an “alarm/locked out” state. This problem is caused by what the switch sees as an abnormal shutdown of the T1 line.
Workaround: Use a dialer interface as the backup interface. This leaves the T1 line alone so that it never goes down, thus avoiding the problem.

- CSCdk55542

The Cisco 3600 series modular access platform might cease to output data on the Ethernet and serial interfaces of the 2E2W combo card. The serial interface might react with a “line protocol down” error and severe output drops on the Ethernet and serial interfaces.

Workaround: A reload temporarily corrects the situation.

- CSCdk64756

The Dynamic Host Configuration Protocol (DHCP) proxy allows the same IP address to belong to two users on different ports with the same username.

Workaround: Ensure that all users have unique usernames.

- CSCdk82279

Authentication using a Vircom RADIUS server stops working after you upgrade to Cisco IOS Release 11.3(6)T1 on a Cisco 5300 series access server.

There is no known workaround.

- CSCdm10611

On a Cisco 3600 series router, the voice quality is degraded by misses in the Real-Time Transfer Protocol (RTP) header-compression.

There is no known workaround.

- CSCdm15208

When Cisco IOS Release 11.3(4)T, 11.3(6)T, or 11.3(7)T is running on a Cisco 2613 router, the following error message scrolls across the log:

```
%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=809E66FC, count=FFFF8093  
-Traceback= 801AF4B4 8057413C 80575764 801BD450 801BCB44 801F0D68
```

There is no known workaround.

- CSCdm29569

A Cisco 7204 router might restart by arithmetic exception tcp_statestring.

There is no known workaround.

- CSCdm30084

A Cisco 2612 router experiences a problem when connecting to a BayStack 504 Hub by way of Bay Networks 354-ST Fiber Extenders.

There is no known workaround.

- CSCdm41484

A Cisco router might restart because of a bus error at cd2430_read_cable_id.

There is no known workaround.

- CSCdm42599

A Cisco 7206 router running the Cisco IOS c7200-ds-mz.113-8.T1 image restarts with the following error:

Software forced crash, PC 0x602F7AB0

The following stack trace decode indicates that memory corruption has occurred:

```
0x602F7AB0:abort(0x602f7aa8)+0x8 0x602F6368:crashdump(0x602f6284)+0xe4
0x602E3008:validblock(0x602e2e48)+0x1c0 0x602E5CD0:validate_memory(0x602e5c50)+0x80
0x602E7A78:checkheaps(0x602e7a10)+0x68 0x602E7CB0:checkheaps_process(0x602e7bd0)+0xe0
0x602DBB74:r4k_process_dispatch(0x602dbb60)+0x14
0x602DBB60:r4k_process_dispatch(0x602dbb60)+0x0
```

There is no known workaround.

- CSCdm63193

If encryption is running on an interface, keepalives are not sent to the other end of the circuit, causing the circuit to fail. Remove encryption statements and the circuit will recover.

There is no known workaround.

- CSCdm67455

A Cisco 7200 series router running an Enterprise image (c7200-js-mz) might experience unexpected reloads.

There is no known workaround.

- CSCdm67456

Running two Cisco 3640 routers might affect the performance of all the analog voice-ports.

Workaround: Reload the routers.

Protocol Translation

- CSCdk84427

In Cisco IOS Release 11.3 running Transmission Control Protocol (TCP) to X.25 protocol translations, translation sessions might be closed prematurely.

There is no known workaround.

- CSCdm32297

A Cisco 2600 series router reloads when translating X.25 to PPP on a vty asynchronous interface that is being cloned from a virtual template. When the router receives a connection and tries to clone the virtual template, the router restarts with a SegV fault in pt_run_vtyslip_ppp_connection.

There is no known workaround.

TCP/IP Host-Mode Services

- CSCdm04532

When two rlogin sessions are made on a router within 1/2 second, one session might send data while the urgent pointer received from the server was intended for the other rlogin session.

There is no known workaround.

- CSCdm27203

A Route Switch Processor in a Cisco 7500 series router might restart with the following error:

```
a Software forced crash, PC 0x601F750 at %TCP-2-INVALIDTCPENCAPS: Invalid TCB encaps  
pointer: 0x0 -Process= "IP Input"
```

There is no known workaround.

Wide-Area Networking

- CSCdk14692

Upgrading to Cisco IOS Release 11.3(3a)T creates an authorization when you try to dial out using ISDN.

Workaround: Turn on authorization for the user.

- CSCdk70002

A Cisco 7500 series router with channelized E1 lines might reload while removing the **channel-group x timeslot y-z command** from the E1 controller. This problem occurs when the associated channel-group serial interface is running Point-to-Point Protocol encapsulation.

Workaround: Shut down the E1 controller with the subcommand **shutdown** when making changes.

- CSCdk85925

Pressing the cancel button when asked for a callback number might terminate a connection.

There is no known workaround.

- CSCdk87679

This caveat occurs when two routers configured to asynchronous dial each other using static dialer maps with PPP encapsulation and PPP authentication CHAP.

The first router dials into the second router and connects. PPP negotiates with no problem and the IP route is installed. The first router pings the second router and fails. The debug IP packet on the first router indicates that the packets have been sent.

Workaround: Remove the **ppp authentication chap/pap** command from either router.

- CSCdk90203

A Cisco 3640 router might reload by a bus error at ClearTimer when running Cisco IOS Release 11.3(7)T.

There is no known workaround.
- CSCdm02785

A Cisco 2600 series router running Cisco IOS Release 11.3 reloads with a SegV exception when you enter the **x25 map cmns** command.

Workaround: Use the equivalent **x25 route** command.
- CSCdm09169

A Cisco 7500 series router running HP OpenView discovery causes the router to reboot.

Workaround: Disable SNMP on the router.
- CSCdm10467

A Cisco 7500 series router with an ATM Interface Processor running Cisco IOS Release 11.3(7)T can reload with the following bus error:

```
System was restarted by bus error at PC 0x6081E95C, address 0xDEADB1F"
```

This output appears after you issue a **show version** or a **show stack** command.

There is no known workaround.
- CSCdm17914

The following caveat occurs on systems containing all of these preconditions:

 - A Cisco 2610 router running Cisco IOS Release 11.3(7)T
 - An eight-port Basic Rate Interface card with ports 0–2 connected over ISDN PPP multilinks to an Internet service provider and ports 3–7 connected for remote users.

ISDN users might experience reloads after connecting to the Internet service provider.

There is no known workaround.
- CSCdm37798

Using PIC code for an international call is tagged as a local call as opposed to an international call; therefore, the ISDN 5ESS switch rejects this asynchronous call.

There is no known workaround.
- CSCdm38034

When a two-port asynchronous/synchronous serial WAN interface card (WIC-2A/S) is configured as asynchronous, it works properly, but does not show up in the running configuration or the startup configuration. However, when configured as synchronous, the serial interfaces appear in the configurations.

There is no known workaround.
- CSCdm41493

A Cisco 2600 series router running Cisco IOS Release 11.3.(9)T reboots when doing an X.25 to TCP translation.

There is no known workaround.

- CSCdm45432
A Cisco 2600 series router running Cisco IOS Release 11.3T might reload due to a SegV exception when a LAN Extender (LEX) interface is enabled.
There is no known workaround.
- CSCdm45941
A Cisco router running TCP to X.25 translation on a X.25 serial link might reload with a bus error.
There is no known workaround.
- CSCdm51011
A Cisco 2610 router running Cisco IOS Release 11.3(9)T connected to a Switched Multimegabit Data Service (SMDS) cloud through a serial interface might experience connectivity problems when fastswitching is enabled.
Workaround: Disable fastswitching.
- CSCdm52131
When **substitute-source** and **substitute-destination** are configured in the same X.25 route statement, the service adapter substitution might be corrupted.
There is no known workaround.
- CSCdm57049
When optimum switching is configured on an RSM/VIP2 Token Ring adapter interface, trace routing through the RSM/VIP2 reports the same next-hop address twice.
Workaround: Use distributed switching on the RSM/VIP2 port adapter interfaces.

Resolved Caveats—Release 11.3(11)T

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

Basic System Services

- CSCdk80230
Certain Internetwork Status Monitor (ISM) NetView users can issue nonenable mode commands without router authentication. Users accessing the router through NetView must be authenticated through NetView's security methods, which may include RACF and SAF. Mainframe users can be restricted from issuing any router commands through the restriction of the RUNCMD within NetView. Users issuing enable mode commands must be authorized to issue this level of command through 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.
There is no known workaround.
- CSCdk90201
The accounting log and the Calling-Station-Id attribute are incorrect in the accounting log.
There is no known workaround.

- CSCdm29567

The **ip trigger-authentication** command is not available on Cisco 1605 routers.

There is no known workaround.

- CSCdm32534

When **vpdn search-order domain** is configured, you might experience the following message, which indicates that a search is done on DNIS and not the domain:

```
Apr 19 18:04:32.572: %VPDN-6-AUTHORERR: L2F NAS APAS5 cannot locate a AAA server for
As19 DNIS 9955555.
```

There is no known workaround.

- CSCdm43731

A Cisco 7513 router might reload when you issue the **aaa accounting periodic timer event**, or **aaa accounting periodic** commands.

Workaround: Remove the **aaa** commands.

DECnet

- CSCdm28939

Configure DECnet on a Cisco 2611 router running Cisco IOS Release 11.3(7)T causes the router to reload.

There is no workaround.

EXEC and Configuration Parser

- CSCdm33057

A MICA line with **flowcontrol software** configured does not properly respond to an XOFF flow control character received from a modem if the line is running an outbound Telnet session. Issuing the **show line** command shows that the line is in the “Waiting for XON” state. The IOS software should wait for an XON flow control character; however, it keeps sending data out the line.

There is no known workaround.

IBM Connectivity

- CSCdm30793

A Cisco 7206 router running Cisco IOS Release 11.3(9)T that is configured for DLSw priority peers might reload with a bus error.

There is no known workaround.

- CSCdm38759

If a Cisco Route Switch Module (RSM) is configured with IBM Spanning Tree, and IP routing is disabled, the RSM does not respond to a single-route or all-route ARP frame destined to its MAC address.

Workaround: Disable IBM spanning tree on the RSM.

Miscellaneous

- CSCdk02130

Initiating a Kerberized Telnet session from a router to a remote host causes the router to reload. This only happens when credential forwarding is configured and when the Telnet session is using a Token Ring interface.

There is no known workaround.

- CSCdk75060

The following caveat occurs on a system with all of the following attributes:

- UNIX client with a locally attached external Nortel Rapport modem (dial-up access analog/ISDN)
- Cisco 3620 router running Cisco IOS Release 11.3(7)T configured for AAA using RADIUS for security

The purpose of this setup is to support virtual private dial-up networking (VPDN). The Nortel Rapport acts as the network access server (NAS), and a Frame Relay connection exists between the Rapport and the Cisco 3620 router. The Cisco 3620 router acts as the home gateway. The caveat occurs when a UNIX client dials into the Rapport and interactively logs in and starts a PPP session. The Rapport never attempts to open an L2F tunnel for the UNIX client. The UNIX client receives a gateway login failed error message from the Rapport.

Workaround: The problem does not occur when the router runs Cisco IOS Release 11.2(15a)P.

- CSCdk86212

A Cisco AS5300 series access server running Cisco IOS Release 11.3(7)T and MICA code 2.6.1.0 will not make two consecutive outgoing calls. Every second outgoing call fails.

There is no known workaround.

- CSCdm11589

A Cisco 3640 NM-4T four-port serial module does not function when a 1FE-1CT1 is in slot 2 and an NM-30DM is in slot 3. This caveat also applies to the HSSI model of the 3640 NM-4T port adapter.

Workaround: Place the 1FE-1CT1 in slot 3 and the NM-30DM in slot 2.

- CSCdm21265

DLSw on the route switch module (RSM) does not operate after you delete remote source-route bridging (RSRB) configurations.

Workaround: Reload the RSM.

- CSCdm28872

Encryption traffic does not bring up an asynchronous dial-up line.

There is no known workaround.

- CSCdm33429

A Cisco AS5300 access server experiences a bus error under heavy load conditions that are caused by outgoing modem calls.

There is no known workaround.

- CSCdm33707

After a Cisco router is reloaded, the data encryption service adapter (ESA) cannot reestablish an active crypto connection.

Workaround: Remove the crpto map, reload the router, and apply the crypto map again.

TCP/IP Host-Mode Services

- CSCdj91130

There is no flow control in RIF passthrough over DLSw. Therefore, if the steady-state traffic on the LAN is greater than the TCP peer connection, the TCP queue can build up above the TCP-queue maximum. This causes the DLSw TCP peer session to fail eventually.

There is no known workaround.

- CSCdk14281

TCP intercept only works with NetFlow switching in watch mode.

Workaround: If intercept mode is required, use either optimum or fast switching.

TN3270

- CSCdm45461

The TN3270 client available in Cisco IOS software does not display local characters that are typed on the screen. System logon continues, and screens appear in the correct sequence, but locally typed characters are not displayed.

There is no workaround.

Wide-Area Networking

- CSCdk87666

When two routers (Router A and Router B) have been configured to asynchronously dial each other using static dialer maps (using the **encapsulation ppp** and **ppp authentication chap** commands), Router A dials Router B and connects. PPP negotiates with no problem and the IP routes are installed. Router A pings Router B but fails. The debug IP packet on Router A shows that packets were sent. The debug IP packet on Router B shows “encapsulation failed.”

There is no known workaround.

- CSCdm05634

A virtual access interface is failing to add packet inputs and outputs of two physical pipes of a multilink PPP bundle connection coming from the same user as an analog call to the asynchronous line of a Cisco AS5200 access server. The client environment is using Windows 98 dial-up networking.

There is no known workaround.

- CSCdm08983

A Cisco 4000 series router restarts with a bus error at PC 0x11A26A, address 0x4AFC4C8A. The router reloads approximately twice a day.

There is no known workaround.

- CSCdm27809

A Cisco RSP2 might reload several times a week with the following error:

```
System was restarted by bus error at PC 0x6024BD28[rsp_aip_fs_body(0x6024a310)+0x1a18],
address 0x2[__start(0x60010000)+0x9fff0002]
rsp_aip_fs_body rsp_process_rawq rsp_qa_intr rsp_aip_fs_body
```

There is no known workaround.

- CSCdm28566

When a PRI interface is configured as a backup interface and a router is reloaded with this configuration, the PRI will not establish layer 2 when the primary interface fails. Set asynchronous balance mode extended (SABME) packets are seen from the switch, but the Cisco IOS software does not respond until the interface is physically reset (that is, you unplug and plug in the PRI cable.)

There is no known workaround.

- CSCdm30090

If you use Erickson X.25 switches and a call is switched on a router using the second address defined in the **x25 route** command, the outgoing call has the facility byte changed and the call is cleared.

There is no known workaround.

- CSCdm31907

Under certain circumstances, a LANE subinterface that is shut down might be reported as “active” from a Hot Standby Router (HSRP) point of view.

There is no known workaround.

- CSCdm34951

AODI might drop the first D-channel link and then drop a B-channel link, but leave a second B channel up.

There is no known workaround.

- CSCdm36139

Incoming calls on a Cisco 2619 router might be cleared, and then the following messages appear:

```
%ISDN-6-NO_TIMER: No Free Timer Entry, caller 0x800AC840, timers used 3839
%ISDN-6-INVALID_TIMER: LIF_RemoveTimer: Invalid Timer Handle, caller 0x800A9DBC handle
-1 %ISDN-6-NO_TIMER: No Free Timer Entry, caller 0x800AC840, timers used 3839
%ISDN-6-INVALID_TIMER: LIF_RemoveTimer: Invalid Timer Handle, caller 0x800A9DBC handle
-1
```

There is no known workaround.

- CSCdm37889

An E1 controller (PRI) might stop responding to the ISDN call setup of a telco switch.

Workaround: Reload the router.

- CSCdm41090

You might observe an ISDN memory leak on a Cisco 4500 central router. When the remote sites go down or the ISDN link drops, the central router repeatedly attempts to dial the remote site. If the connection is not established, the central router keeps dialing and eventually runs out of memory and reloads.

Workaround: Reboot the router.

- CSCdm43734

A Cisco router that is configured for Dialer Watch needs to call the remote end because of failing watched routes. If the call is unsuccessful for any reason, the router never attempts to dial out. No attempt is made, even when the route has been restored or removed.

Workaround: Reload the router.

- CSCdm44902

A Cisco 2600 series router with a Cisco Multiport Basic Rate Interface (MBRI) cannot place outgoing calls because “No free dialer” is reported even if the dialer is idle.

There is no known workaround.

Resolved Caveats—Release 11.3(10)T

All the caveats listed in this section are resolved in Release 11.3(10)T. This section describes only severity 1 and 2 caveats.

Access Server

- CSCdm00811

Malloc failures might be seen on a Cisco AS5300 access server when virtual templates are configured under heavy stress conditions.

Workaround: Configure the input hold queue size on the virtual template to 10.

- CSCdm09417

A Cisco AS5200 access server might not be able to dial out using channel-associated signalling (CAS). This condition occurs intermittently.

There is no known workaround.

- CSCdm21330

When you change the maximum transmission unit (MTU) from the default settings on a serial interface in High-Level Data Link Control (HDLC) mode on the channelized group of a four-port E1 controller, the serial interface goes into the administratively shut down state.

Workaround: Use an eight-port E1 controller.

- CSCdm22177

T1 timeslots can become blocked and they cannot be reinstated without reloading the router. The problem occurs under extremely heavy traffic conditions, with a switch placing calls on timeslots within 800–900 ms of clearing a prior call. The call logs show some calls placed by the switch being cleared within 40 ms of the seizure.

Workaround: Check whether the counter is negative and treat it as “0” available timeslots. The race condition itself is handled by the CSM state machine. All states have protocol timeouts to handle this type of situation.

Basic System Services

- CSCdk59010

If you use reverse Telnet to a binary Telnet port with RFC-2217 COM port extensions, and if you make multiple successive dialouts from a single Telnet session, after several outgoing calls, the Cisco IOS Telnet server prematurely sends a FIN to the RFC-2217 client.

There is no known workaround.

IBM Connectivity

- CSCdm21529

A Channel Port Adapter (CPA) might not recover from a fatal error reload. This requires that you manually reload the microcode for this card. While in this mode, if you enter the **show running** or **write term** commands, the console locks up and displays the “SCHED-3-THRASHING” error message.

Workaround: After a CPA fatal error, if the card does not restart, issue the **microcode reload** [*ecpalpcpa*] **slot** *n* command to reload the microcode for the card having problems. If you get the “SCHED-3-THRASHING” error message, Telnet to the router on a different vty and perform the microcode reload there.

Interfaces and Bridging

- CSCdk67709

Multilink PPP interleaving causes a delay in outbound traffic on RSP platforms.

There is no known workaround.

Miscellaneous

- CSCdk75285

When a Certificate Revocation List (CRL) size is larger than 2K, the router might reload.

Workaround: Have a smaller CRL issued from the server.

- CSCdk85615

There is no method of configuring MICA modem lines for dial-out only on a Cisco 3640 router. The **modem-dtr-active** command fails with a “no dialtone” message.

There is no known workaround.

- CSCdk93483

If voice traffic is process-switched (for example when using RTP header-compression), the execution of certain EXEC commands on the router (**show running-config**), can have an adverse effect on the quality of voice calls during the execution of the command when it is competing with voice packets for CPU time.

There is no known workaround.

- CSCdm08139

In Cisco IOS Release 11.3(8)T1, a Cisco router running 56-bit encryption and configured to run IPsec over a Frame Relay Point-to-Point circuit fails. The packets from the source IP address are dropped at the router configured for IPsec.

There is no known workaround.

- CSCdm08728

A router running Cisco IOS Release 11.3(6)T might experience unexpected system restarts when configured with crypto IPsec commands when receiving Cisco Encryption Technology (CET) connection messages.

Workaround: Add an access control list (ACL) statement to explicitly deny the connection message.

- CSCdm17363

A Cisco 2610 router reloads with a SegV exception in ccGetCall Active.

There is no known workaround.

- CSCdm19275

On a Cisco 7200 series router, the Channel Port Adapter with a microcode version of 26.0 or later might reload with the following error message:

```
%XCPA-3-OUTHUNG: Channel12/0 - output stuck - resetting %ECPA-2-MSG: slot2 %XCPA-2-MBX:  
Force dump requested -0
```

There is no known workaround.

- CSCdm19926

If mismatched access control lists (ACLs) are used in crypto maps—that is, one side of the crypto connection has an ACL statement that the other side lacks—existing crypto connections might stop working.

There is no known workaround.

- CSCdm24281

A Cisco router configured for Director Response Protocol (DRP) might reload with the following error message:

```
spurious memory access
```

There is no known workaround.

- CSCdm38247

Voice ports on Cisco 3600 and Cisco 2600 series routers might become disabled after you reload the router. This condition occurs when either input gain or output attenuation is configured under the voice port. The symptom of this problem is that when the port is “off-hook,” the dial tone is not detected. Also, the operational state shows “DOWN,” as seen with the **show voice port** command.

Workaround: Remove the gain or attenuation from the voice port, save this change to NVRAM with the **copy running-config startup-config** command, and reload the router. After the router reloads, enter the voice port gain or attenuation configuration back in.

- CSCdm39334

Crypto (CET and IPSec) might fail when keys expire or are cleared over a tunnel interface.

There is no known workaround.

Wide-Area Networking

- CSCdk68549

A Cisco router might reload when the **no dialer remote-name** [*name*] command is issued and the router is actively trying to dial the named remote site.

Workaround: Issue the **shutdown** command from the configure interface mode before issuing the **no dialer remote-name** [*name*] command.

- CSCdk76245

Cisco access servers configured for Always on Dynamic ISDN (AODI)/X.25/BAP/MPPP with the **ppp multilink idle-link** command might cause a problem for non-AODI clients using MPPP.

The MPPP client, when connected with more than one B channel, has the first channel in receive mode and the other channels belonging to the same bundle in normal mode.

There is no known workaround.

- CSCdm06415

The dial-on-demand routing test fails over a BRI on Cisco 3640 and Cisco 7200 series routers. Pings fail over the BRI with a “no free dialer” message.

There is no known workaround.

- CSCdm22162

Stac compression LZS Digital Control Protocol (DCP) gets into an “R-Req” loop. This problem occurs when you run Cisco IOS Release 11.1 or Release 11.2 hardware compression and an RSP on one end of a connection, and Release 11.3 or Release 12.0 software compression on the other.

Workaround: Disable compression if you are using a Cisco 7500 series router. If you are using a non-RSP router, use software instead of hardware compression on both sides, or disable compression.

- CSCdm38212

Outgoing calls fail on routers with PRI interfaces when the switch is NI2.

There is no known workaround.

Resolved Caveats—Release 11.3(9)T

All the caveats listed in this section are resolved in Release 11.3(9)T. This section describes only severity 1 and 2 caveats.

Access Server

- CSCdk89339

On a Cisco AS5300 series access server with a quad computer telephony integration (CTI) card, with a channel associated signaling (CAS) T1 configured for Extended Superframe/binary 8-zero substitution (ESF/B8ZS) e&m-fgb signaling, the telco might force our CSU to go into loopback mode, killing NEAT.

Workaround: Reload the access server.

Basic System Services

- CSCdk38555

When using RADIUS authentication for dial-in PPP users, the router might reload after one or more calls.

Workaround: Remove the AAA accounting configuration.

- CSCdk69378

A Cisco 1600 router with IP configured might experience leaks in the I/O memory area. This condition might cause the router to reload.

There is no workaround.

- CSCdk81029

On the IOS firewall of a Cisco 1600 series router, “ASSERTION FAILED” and “%QUICC-3-OWNERR” error messages are received at boot time.

There is no workaround.

- CSCdk88213

A Cisco AS5200 series access server running AAA accounting in Cisco IOS Release 11.3(7)T might reload by a bus error.

There is no known workaround.

IBM Connectivity

- CSCdk83457

On a Cisco 7200 series router running Cisco IOS Release 11.3(7)T, invalid Transmission Control Protocol (TCP) encapsulation errors might occur.

There is no known workaround.

- CSCdk89189

A Cisco 2600 series router configured with a DLSw priority backup peer configured for Basic Rate Interface (BRI) might reload with a SegV exception.

Workaround: Avoid configuring the priority keyword on DLSw.

- CSCdk51086

When Qualified Logical Link Control (QLLC) is used as a transport mechanism for SNA traffic, X.25 might get stuck in “Receiver not Ready” (RNR) when the input queue is full.

Workaround: Increase the capacity of the input queue to 1000 packets.

Interfaces and Bridging

- CSCdk85541

A Route Switch Module (RSM) running Cisco IOS Releases 11.3(5)T through 11.3(7)T will not route an IP frame through a Token Ring VLAN with transparent bridging enabled.

Workaround: Configure Integrated Routing and Bridging (IRB) on the Token Ring VLAN and router IP frames to the Bridge Group Virtual Interface (BVI).

- CSCdk70579

The user might see collisions accumulating on a Cisco 3600 Fast Ethernet interface configured for full-duplex (fdx).

Workaround: Configure the interface for half-duplex (hdx).

Miscellaneous

- CSCdj82823

A Cisco 7200 series router configured to route IP packets over ISDN with encryption works only in process-switch mode.

Workaround: Disable fast switching.

- CSCdk29352

RADIUS attribute 61 is missing in Release 11.3(4.4)T.

There is no known workaround.

- CSCdk89767

A channelized E1 interface on a Cisco 3600 series router might not be able to transmit data when multiple timeslots are associated with a channel group. The problem manifests itself in keepalive failures and line protocol down indications.

Workaround: Reload the router or break the channel group into smaller groups.

Novell IPX, XNS, and Apollo Domain

- CSCdk83756

Using Internetwork Packet Exchange (IPX) in conjunction with virtual templates on a Cisco 3640 router does not work.

Workaround: Change the IPX network number on the virtual template on the sending and receiving sides of the routers and restart Point-to-Point Protocol (PPP).

Protocol Translation

- CSCdk67438

When you run Cisco IOS Release 11.3 and use TCP to X.25 permanent virtual circuit (PVC) protocol translation, the PVC might close too quickly. This could potentially cause the PVC to be taken down prematurely, causing data to be lost. When you print over TCP-to-X.25 PVC protocol, the translation might experience a loss of the last data blocks.

There is no workaround.

- CSCdk53971

The user is unable to get Resource Reservation Protocol (RSVP) to set the appropriate weight in weighted fair queuing (WFQ) to achieve the proper quality of service for video file transfers.

Workaround: Avoid configuring RSVP on subinterfaces.

Wide-Area Networking

- CSCdk70741

The line protocol might flap under these conditions:

- Two connecting routers, both running Cisco IOS Release 11.3(6)T using Point-to-Point Protocol (PPP).
- A PPP reliable link is being utilized.

There is no known workaround.

- CSCdk76478

When you run Cisco IOS Release 11.3 while performing a TCP-to-X.25 SVC translation, the M bit might not be set on outgoing packets apart from the same datagram. When the TCP data stream and datagrams are above the limits of the packet size on the X.25 portion, a payload is incorrectly interpreted as a separate packet although they are part of the same datagram.

There is no workaround.

- CSCdk77947

A Cisco AS5200 series access server running AO/DI in Cisco IOS Release 11.3(6)T1 might reload with an unexpected interrupt message.

There is no workaround.

- CSCdk45052

This problem was found in a Cisco AS5300 running Release 11.3(5.1)T with four T1/PRI lines configured for NFAS Digital MICA modems running portware version 2.3.1.0 and the Enterprise feature set. All inbound calls for ISDN and analog work correctly. The problem occurs when you reverse-Telnet into a rotary (which the MICA modems are in for dial-out use). The first reverse-Telnet and outbound call works correctly; however, each of the following outbound calls (as long as the first call is still up) fail until the first call is dropped. It appears that a B channel is not being allocated. After a few minutes, the call times out and the modem is de-allocated.

There is no known workaround.

- CSCdk86188
ISDN might not operate properly and give an “isdn_check_dialer failed” message.
There is no known workaround.
- CSCdk45469
Microsoft callback over ISDN might cause the router to reload.
There is no known workaround.

Resolved Caveats—Release 11.3(8)T

All the caveats listed in this section are resolved in Release 11.3(8)T. This section describes only severity 1 and 2 caveats.

Access Server

- CSCdk68655
A Cisco router might periodically reload (approximately every 2 hours) with a bus error. The resulting error message is:

```
System restarted by bus error at PC 0x2252987E, address 0x4AFC5A80
```


Workaround: Replace the controller E1 card.

Basic System Services

- CSCdk59328
When you use a Cisco router to dial in to a Cisco AS5300 access server, the Cisco AS5300 might not force the router to receive an address from the Dynamic Host Configuration Protocol (DHCP) server. This condition might occur if the access server is using both authentication, authorization, and accounting (AAA) and the peer default IP address.
There is no known workaround.
- CSCdk66007
A Cisco 2600 series router might reload by SegV exception at “rlogin_open_connection.”
There is no known workaround.
- CSCdk67339
When a Cisco 1600 router is connected in Synch mode using the Easy IP feature, the WIC-1T sync/async might drop the PPP link. This condition is caused by having **ip address negotiated** configured on the serial interface. When a static IP address is configured, the problem does not occur.
There is no known workaround.

- CSCdk59099

AAA connection accounting works for a single connection on the router, but with multiple connections start records are generated for all connections, but only the first disconnected call has a stop record generated; subsequent closed connections do not. All records have the same Acct-session-id. This problem exists in Cisco IOS Release 11.3(2.4)T or later.

There is no known workaround.

Interfaces and Bridging

- CSCdk58144

You cannot successfully ping packets or copy files between Microsoft NT servers.

There is no known workaround.

Miscellaneous

- CSCdk42284

When an Foreign Exchange Office (FXO) port is configured for private line auto ringdown (PLAR) to make it ring a Foreign Exchange Station (FXS) station across IP or on the same router, the FXS station (Tel2) sometimes continues to ring even when the call is disconnected by the caller (Tel1). This problem occurs 50 percent of the time even with “no supervisory” at the FXO.

There is no known workaround.

- CSCdk43602

Bell103 does not work on analog Microcom modems in answer mode. This problem is related to the analog modem firmware that is bundled with the Cisco IOS. When this problem is resolved, you need to upgrade your analog modem firmware.

There is no known workaround.

- CSCdk55307

A Cisco 3640 router using ISDN BRI interfaces might reload.

There is no known workaround.

- CSCdk60026

A Cisco 2610 router configured with SDLC DLSw+ might not send SNRM frames to a terminal even though the status is “SNRMSSENT” in the output from the **show interface serial** command. The interface shows “Link is UP, Line protocol is UP” despite the DTR being down.

Workaround: Execute the **shutdown** command followed by the **no shutdown** command in configuration mode for the serial interface.

- CSCdk65683

A Cisco 2600 series router might experience physical (checksum) errors on the Ethernet network between a Cabletron ELS10 (store and forward) Ethernet switch and the 10BaseT port. This condition occurs when you try to ping from a PC on the other side of the Cabletron switch to the router.

There is no known workaround.

- CSCdk27524
Fax over IP over Token Ring might experience failure with long fax jobs (for example, after about 5 to 10 pages).
There is no workaround.
- CSCdk59879
A Cisco 1600 router or Cisco 3600 series router reloads when IPSec is configured over the ISDN link. This condition is caused by the IP route-cache that is enabled by default on all interfaces.
There is no workaround.
- CSCdk68107
A Cisco 2600 series router might reload by SegV exception approximately once per hour.
There is no workaround.

Wide-Area Networking

- CSCdk61807
When you perform an ISDN callback, you might receive the following message:

```
%SYS-3-HARIKARI: Process ISDN top-level routine exited
```


There is no workaround.
- CSCdk60097
On a Cisco AS5300 running Cisco IOS Release 11.3(6.1)T with an IP plus feature set, the global command **modem busyout-threshold xx** cannot place B channels in or out of service on a non-facility associated signalling (NFAS) line without a D channel (the line is neither a primary nor a backup NFAS line).
There is no known workaround.
- CSCdk66465
A Cisco AS5200 series access server might reload at a high CPU range, causing all users to be disconnected. The resulting bus error message is:

```
System was restarted by bus error at PC 0x2252A6F0, address 0xD0D0D0D 5200 Software  
(C5200-I-L), Version 11.3(6)T1, RELEASE SOFTWARE (fc1) Compiled Fri 16-Oct-98 01:43 by  
ccai (current version) Image text-base: 0x2202DF90, data-base: 0x00005000
```


There is no workaround.
- CSCdk67475
Under heavy usage conditions on an X.25 serial link, a Cisco router running translated X.25 to virtual async connections (PPP/IPX) might reload. This appears to be an infrequent occurrence.
There is no known workaround.
- CSCdk69509
An RSP2 on a Cisco 7500 series router might crash with a bus error. This condition is related to X.25 and Link Access Procedure, Balanced (LAPB).
There is no known workaround.

- CSCdk67735
VPDN does not support MS-CHAP.
Workaround: Use CHAP or PAP.
- CSCdk69497
A Cisco router might fail with a memory leak after about a week of running or 12,000 modem calls. The resulting error message is: `ISDN NLCB allocation failed`.
Workaround: Reloading the router clears the condition.

Resolved Caveats—Release 11.3(7)T

All the caveats listed in this section are resolved in Release 11.3(7)T. This section describes only severity 1 and 2 caveats.

Access Server

- CSCdk20217
A Cisco 5300 series router or Cisco 5200 series router might reload as a result of “assertion failures.”
There is no known workaround.

Basic System Services

- CSCdk47382
The Network Time Protocol (NTP) on Cisco 2600 and Cisco 3800 series routers does not stay synchronized. After approximately five minutes the clock wanders and the NTP becomes unsynchronized. Removing the NTP configuration and adding the NTP configuration back causes the router to synchronize again, but later it becomes unsynchronized.
Workaround: Configure the NTP clock period as: **`ntp clock-period 17208078`**.
- CSCdk48674
The Cisco 1600 series router is not able to receive multicast packets for different groups at wire speed. This causes the Cisco 1600 Ethernet driver to miss packets.
Workaround: Configure static multicast groups.

Miscellaneous

- CSCdk19122
When the CT1-PA and the CE1-PA are configured for **compress stac**, with the CSA-PA (hardware compression PA) on a Cisco 7206 router, memory leakage in the pool manager might occur. When available memory runs below 1 megabyte, the router might reload.
There is no known workaround.

- CSCdk29115

When you configure Binary Synchronous Communication Protocol (Bisync) using the **encapsulation bstun** command with the ASCII character set (**bsc char-set ascii**) on the first port of a serial WAN interface card (1T, 2T, or 2A/S) in WIC slot 0 of a Cisco 2600 series router, only the first character of each frame is received, and the Block Serial Tunneling (BSTUN) tunnel is not established. This only affects Bisync mode when it is configured with the ASCII character set. Other encapsulations are not affected, and using the EBCDIC character set with Bisync works correctly.

For the first serial port in WIC slot 0, the parity detection is not configured correctly for Bisync in ASCII mode. The first character of each frame generates a parity error that causes the receiver to discard the frame after the first character received.

Workaround: Use a different serial port: either the second serial port (port 1) on a 2T or 2A/S WIC in WIC slot 0 or any serial port in WIC slot 1. If you have only one serial WIC, moving it from WIC slot 0 to WIC slot 1 fixes this problem.

- CSCdk46537

The length field in the MAC management message header for the “SYNC” message is computed incorrectly. This was found during testing with the Cadence CM at Cable Labs.

Workaround: Use a modem that has the Broadcom chipset. Because the “SYNC” message is a well-known size, the Broadcom chipset can read the Cable Modem Termination System (CMTS) timestamp without looking at the length field.

- CSCdk48214

When using MS-CHAP with RADIUS, the Cisco IOS software might deliver malformed packets. However, RADIUS implementation for MS-CHAP should comply with the latest specification from Microsoft.

There is no known workaround.

- CSCdk49622

After a Cisco 3600 series router or Cisco 2600 series router is power cycled, the ATM25 Network Module stops transmitting packets.

Workaround: Use any other image before Cisco IOS Release 11.3(5.1)T and Cisco IOS Release 12.0(2)T or after Cisco IOS Release 11.3(6)T and Cisco IOS Release 12.0(1)T.

- CSCdk49638

Generic traffic shaping does not work on the Ethernet interface of a Cisco 2600 router.

There is no known workaround.

- CSCdk51554

The VPM ports of a Cisco 3600 router might fail. The resulting error message:

```
42-1-NO_RING_DESCRIPTOR: No more ring descriptors available on 3 slot
```

Workaround: Reload the router to recover the voice ports.

- CSCdk54726

A Logical Link Control type 2 (LLC2) connection request coming from a TRISL trunk and passing by means of a DLSw might experience a failure. Debug DLSw indicate “DLSw sap entry invalid.”

Workaround: Configure multiring on the Fast Ethernet subinterface.

- CSCdk56104

When a router is booted, the following traceback might appear: “Process= “CCVPM_VCSM,” followed by a traceback message. Some VPM ports become unusable as a result.

There is no known workaround.

- CSCdk58500

If a ground-start link is initiated by the FXO port of a Cisco 3600 router, the secondary dial tone returned by the connecting FXS port does not get passed through to a handset connected to the loop-start FXS port of the Cisco 3640.

There is no known workaround.

- CSCdk59049

When you run TR-ISL to a Cisco 7000 family router, some frames larger than 1535 bytes might not be forwarded. This condition occurs when you run TR-ISL between two VLANs that are on switches.

Workaround: Do not use TR-ISL. Use an external device to router or bridge between the two different VLANs. Or modify the end devices so that they do not send packets larger than 1500 bytes.

Wide-Area Networking

- CSCdk28918

MS callback server functionality in Cisco access servers is not working with configurations involving async/ISDN interfaces configured with dialer profiles.

There is no known workaround.

- CSCdk51087

Running Always on Dynamic ISDN (AODI) with a deactivated ISDN line might cause an I/O memory leak.

There is no known workaround.

- CSCdk62967

Cisco 2600 series routers with ISDN configurations (both BRI ISDN and PRI ISDN) interfaces might reload with a watchdog timeout when the ISDN interfaces are active or operational. This problem occurs only on Cisco 2600 series routers running Cisco IOS Release 11.3(6.2)T and later, Release 12.0(1), and Release 12.0(1)T.

There is no known workaround.

- CSCdk64220

Test frames with a VMAC address respond with the burned-in address as the source address. This is a protocol violation.

There is no known workaround.

Resolved Caveats—Release 11.3(6)T

All the caveats listed in this section are resolved in Release 11.3(6)T. This section describes only severity 1 and 2 caveats.

Access Server

- CSCdk20428

Busying out of all modems simultaneously with the **modem busyout** command can cause active calls to drop.

There is no known workaround.

- CSCdk30581

This problem occurs when Multiservice IOS Channel Aggregation (MICA) runs out of buffers (prints out NO_BUF messages on console) and many EXEC sessions are running. This problem has been observed with the latest 56K modems.

There is no known workaround.

- CSCdk38665

When you configure a channel group, unconfigure the channel group, and then configure a PRI group with Release 11.3 T, a bus error occurs.

There is no known workaround.

Basic System Services

- CSCdk20606

The “tty daemon” process might use a large percentage of the available CPU if large amounts of data are sent to an asynchronous port over a telnet connection (port 20xx, 60xx, and so on).

Workaround: Historically, the workaround has been to use a TCP stream mode connection instead (port 40xx, and so on). However, because new features like FAX dialout require the telnet protocol for proper operations and sends large amounts of data, this process needs to be made more efficient.

- CSCdk41795

The **aaa accounting nested** configuration command is not available from the configuration parser.

There is no known workaround.

Interfaces and Bridging

- CSCdk15786

AppleTalk does not come up on the 2E-FDX interface. The problem occurs only on the 2E-FDX interface.

There is no known workaround.

IP Routing Protocols

- CSCdk20190

A problem exists with a **conf [net | term...]** redeclaration of the dialer interface’s IP unnumbered status, causing all associated routes to disappear. If a group of people are connected to a Cisco 3640 through ISDN over a multilink dialer setup with RADIUS learned routes and the **conf**

term interface dialer1 ip unnumbered loopback 0 ^Z command is entered, the router loses all connected dialer routes and the larger RADIUS learned routes associated with these dialer routes. Using **conf net** also causes problems on the network.

This problem is found in Releases 11.3(1.5) and 11.3(3a)T. It was working on Release 11.2.

There is no known workaround.

- CSCdk26867

On a Cisco 2600 series router running the c2600-is-mz_113-3a_T1 image and the Network Address Translation (NAT) protocol, NAT works until the translation table times out.

Workaround: Only a reload of the router every 24 hours resolves the problem.

Miscellaneous

- CSCdj84663

When using RSVP for Voice over IP (VoIP) on Cisco 3600/2600 series routers (to make bandwidth reservations through the network routers of different platforms), the bandwidth reservations are not granted by the intermediate routers. However, it succeeds between the peripheral VoIP originating and terminating routers.

There is no known workaround.

- CSCdk17038

The router reloads when configuring the **crypto key** and **named-key** commands. The router boots up after the reload, but it does not load the configuration from NVRAM even though the config register is set to 0xE002.

There is no known workaround.

- CSCdk24418

Sometimes the modemcap defined for a modem might not be applied to the modem before allocating the modem for a new call.

There is no known workaround.

- CSCdk27818

Voice over IP calls cause the router to reload if PPP Multilink is enabled on the BRI interface.

Workaround: Force a UDP checksum on the dial peer or remove the PPP Multilink.

- CSCdk29445

The Cisco uBR7200 series cables router, when receiving the registration request, tries to verify the MIC using the algorithm in RFC 2104. If this fails, it tries the method defined in RFC 1321.

Workaround: Create the modem configuration file using a config file editor that uses RFC 1321 to generate the MIC.

- CSCdk31935

When using source router translation bridging (SRTLb) between a TR-ISL VLAN of a source route bridging domain and a TR_VLAN of a TB domain with source route bridging fast switching (default) enabled, the Cisco 7200 TR-ISL router reloads; however, process switching works with the **no source-bridge explorer-fastswitch** command configured.

Workaround: Use process switching.

- CSCdk32041

A system configured for VPDN multihop reloads in “12f_destroy_mid” if the tunnel fails to open to the next hop. This occurs because CSCdj95477 is missing from Release 12.0.

Workaround: Issue the **no vpdn multihop** command.
- CSCdk34205

If you are using NFAS with a backup D channel and the primary D channel goes down, modem calls might fail to be accepted into the access server. Enabling the **debug modem csm** command displays the “dchan_idb state is not up” error message.

There is no known workaround.
- CSCdk36373

RADIUS authentication requests might not include the NAS-Port attribute. This could be a problem if the RADIUS server requires the presence of NAS-Port.

There is no workaround.
- CSCdk38133

The **cablelength** configuration command for the CT1 module is missing in the Cisco 2600 platform for Release 11.3T.

There is no known workaround.
- CSCdk39922

When attempting to dial out on a Cisco 3600 using the digital modems and a single port T1 Network Module, the outbound call fails with “No Answer.” Inbound calls function correctly. Outbound dialing with T1 CAS and a dual-port T1 Network Module works correctly.

There is no known workaround.
- CSCdk41902

When a TR VLAN is configured on an RSM, an IP client might not be able to ping the RSM in the following circumstances:

 - The IP client sends an ARP without a RIF and sends an ARP with a RIF
 - The concentrator relay function (CRF) that the client is connected to is configured for source-route bridging

Workaround: Change the CRF mode from source-route bridging to source-route transparent.
- CSCdk44137

This problem causes the Explorer bit in the TRISL header to be set for non-specific routed (NSR) frames. Normally, the Catalyst 5000 and 3900 ignore this bit for NSR, but sometimes it causes some problems. IP pings for NSR frames fail at times.

There is no known workaround.

Novell IPX, XNS, and Apollo Domain

- CSCdk37063

IPX fastswitching for remotely connected IPX networks is not functioning on the RSM for TR VLANs. When the RSM receives an IPX packet from a TR VLAN that is destined for an IPX network other than that configured on the local interface, it stores an invalid IPX route cache

entry in the route cache. The first IPX frame gets process-switched and works correctly. For the second IPX frame and subsequent frames, the IPX route cache is used to fast-switch the packet, which results in sending out an invalid frame, so the packet never reaches its destination.

Workaround: Disable IPX fast switching by using the **no ipx route-cache** command on the TR VLAN interface of the RSM.

Wide-Area Networking

- CSCdj93845

During the software reload and initialization, the router accesses an uninitialized pointer causing a reload. This problem was found in the c7200-boot-mz image for Release 12.0(0.x) and Release 11.3(2.4)T only. Release 11.3(x) and later do not experience this problem.

There is no known workaround.

- CSCdk24337

MS Windows 95 and MS Windows NT machines dial in and request a callback. The callback is made by the Cisco access server, but the client PC does not answer the returned call. Another symptom is that the client still seems to be negotiating PPP/MS-CB for the first client dial-in connection.

A careful inspection of assorted dial debug logs indicates that the last Terminate Request sent by the client was answered by the Cisco access server. But the access server proceeded to disconnect and return the call immediately. This did not allow time for the last Terminate Ack to make it safely to the client. PPP connection tracing on the client end reveals further clues about this problem.

This problem happens both on ISDN and async connections.

There is no known workaround.

- CSCdk32672

The use of PPP over ATM or PPP over FR causes the system to restart.

There is no workaround.

- CSCdk45571

Cisco 1005 images would not build with the -Y option.

There is no known workaround.

Resolved Caveats—Release 11.3(5)T

All the caveats in the section are resolved in Release 11.3(5)T. This section describes only severity 1 and 2 caveats.

Access Server

- CSCdk00838

You might encounter the following situation with a Cisco 5200 with two T1s that are configured with T1 0 as the primary clock source and T1 1 as the secondary clock source. The problem arises when the controller with the primary clock source goes down. The circuits are connected to a DACCS all of the time and cross connected to the local loop that then goes to the Cisco AS5200.

The problem is that when you disconnect the cable from the router, the clock source switches as advertised. However, when the circuit is unmapped in the DACCS (with the cable still in the router), the remaining circuit cannot pick up the clock. There are errored seconds and slips.

Workaround: Unplug the circuit from the router when it is not being used.

Basic System Services

- CSCdj91329

When the **show ip bgp** command displays routes, the router reloads.

There is no known workaround.

Miscellaneous

- CSCdk01436

If the Cisco uBR7200 series router is overloaded with downstream traffic for more than 30 seconds, all attached modems reset and restart initial ranging. This happens only if there is downstream traffic.

Workaround: Do not overload the system in the downstream direction. A constant overload for that amount of time has only been observed when a packet generator is used to send traffic in the downstream direction only, without a feedback mechanism that also sends data in the upstream.

This condition should never happen in the field, unless the system is overloaded on purpose using a packet generator or an equivalent tool. Normal data transfers, such as FTP or Web traffic, cannot produce this condition.

- CSCdk01958

The **full-duplex** command does not work on the 1FE port adapter.

There is no workaround.

- CSCdk12090

The commands **crypto cisco key-timeout**, **crypto cisco connections**, and **crypto cisco entities** are not recognized by the router.

There is no known workaround.

- CSCdk14486

If the Cisco uBR7200 series is in overload condition, ranging response messages are not sent. This can cause modems to disconnect if the condition lasts longer than 30 seconds. This condition usually only happens in a test environment, where a large number of packets are sent downstream.

Workaround: Do not overload the system with a packet generator. If this condition happens in the field, reduce the number of active modems on a single downstream.

- CSCdk14757

Under the following conditions, a Cisco uBR7200 series system resets:

- The system is polled from an SNMP management system.
- A modem card (MC11) is pulled.

Workaround: Never do both SNMP and OIR (online insertion and removal) of an MC11 card.

- CSCdk15697

Data packets to a cable modem or its associated hosts are encrypted even when privacy is enabled for the cable modem.

There is no workaround. Packets are always sent unencrypted.
- CSCdk17585

Under certain conditions, the MC11 hardware can deliver corrupted data to the system. This can cause various kinds of system reloads.

There is no safe method of detecting if this problem exists in a given system. Analysis to determine if it is caused by a hardware problem is underway.

Workaround: Because it was observed with one specific MC11 modem card only, replace the card.
- CSCdk23293

The BRI interface might not recover if the switch initiates a loss of Layer 1 service.

Workaround: Performing the **shutdown** command followed by a **no shutdown** command on the affected interface might clear this problem. If the problem is not cleared, you might need to reload the router.
- CSCdk26815

When running half-duplex SDLC over a WIC-1T, WIC-2T, or WIC-2A/S interface on a Cisco 2600 series router, the router does not recognize changes in the Clear to Send (CTS) or Ready to Send (RTS) signals on the line. This only affects full-duplex SDLC; full-duplex SDLC works on these interfaces.

There is no known workaround.
- CSCdk26860

When operating with a WIC-BRI-S/T or WIC-BRI-U in one WIC slot and a WIC-1T, WIC-2T or WIC-2A/S in the other WIC slot, the BRI WIC interface does not pass any data traffic. The BRI calls come up, but they drop after 22 to 23 seconds. The BRI WIC works correctly if there is no WIC-1T, WIC-2T, or WIC-2A/S installed.

There is no known workaround.
- CSCdk37323

When a TR VLAN on the RSM is configured for multiring, the router never sends a local test frame without a RIF to the LAN. Because of this, the packet leaving the RSM to the local station contains a RIF that is populated with the pseudo ring CRF, the BRF, and the Catalyst 5X00 TR port CRF. If the station on the ring does not have support for source route bridging enabled, a connection cannot be established.

Workarounds:

 - Turn off multiring by configuring **no multiring all** on the RSM TR VLAN interface. source route bridging devices located behind another Source Route Bridge connected to that ring will now be unable to communicate. However, locally attached stations will now function.

or

 - Enable the source route bridging capability on the affected devices on the ring.

Wide-Area Networking

- CSCdk19188

When callback is used with virtual profiles, users who are configured to not be called back fail to connect.

Workaround: Force the user to request callbacks when callback is configured.

- CSCdk24063

Configuring LES on the main ATM interface on an RSP causes cyBus errors.

There is no known workaround.

Resolved Caveats—Release 11.3(4)T

All the caveats in this section are resolved in Release 11.3(4)T. This section describes only severity 1 and 2 caveats.

Access Server

- CSCdj91500

When using the Cisco AS5300 in the following arrangement you might see a software forced reload when the access server accepts incoming analog calls:

- E1/R2 signaling
- Channel Associated Signalling (CAS)
- Analog modems

This problem has been seen in the following releases: 11.2(11)P, 11.2(12)P, and 11.3(2)T.

Workaround: Configure **dnis-digits x** under **cas-custom**, where the **x** is the number of DNIS digits expected from the control office switch in a range of $0 < x < 66$.

- CSCdj92679

R2 custom configuration does not take effect.

There is no known workaround.

- CSCdk00093

When using E&M FGB signaling on a Cisco AS5200 or Cisco AS5300 with MICA modems, the router does not correctly transmit an off-hook sequence to the network.

Workaround: Use a PRI.

Basic System Services

- CSCdk06447

Authorization method lists that contain methods after “local” fail with a syntax error. This might cause authorization method lists in the configuration to be removed after upgrading to Release 11.3(3)T or later. This might allow unauthorized users into the router and/or cause services not to be automatically enabled for users.

Workaround: Temporarily remove the “local” method from the beginning of the authorization method list.

IP Routing Protocols

- CSCdj80554

When a Cisco 4500 receives ISL packets with a destination MAC address of the form xxxx.xxxx.xx1x, they are not forwarded.

Workarounds:

- Avoid such MAC addresses. They can arise because of the default MAC address on the interface or because Hot Standby Router Protocol (HSRP) uses a virtual MAC address of that form.
- Change the default MAC address with the **mac-address** interface command. Avoid using standby groups between 16 and 31.

Miscellaneous

- CSCdj80895

Under certain circumstances, if fast switching is enabled using the Cisco IOS context-based access control to inspect TCP, the router might reload.

There is no known workaround.

- CSCdj85289

Receiving data while running encryption on a Cisco 2600 series router running Cisco IOS Release 11.3(3)T causes the router to reload.

There is no workaround.

- CSCdj93060

The router might reload when you try to ping with large MTU sizes.

Workaround: Use the default 1500 MTU size.

- CSCdj93893

The Cisco 4500 might stop operating during regression test. The problem cannot be replicated manually and it occurs intermittently.

There is no known workaround.

- CSCdk02511

If the cable modem sends a partial class of service (CoS) configuration in the registration request, the CMTS (Cable Modem Termination System) uses uninitialized values for the unsent CoS parameters. This can cause drastic consequences depending on which CoS parameters were not configured for the modem.

An example of a drastic case is when the “max_tx_burst” for the modem gets set to a very small value. In this case, the modem does periodic ranging correctly, but might experience an upstream deadlock because of the CMTS rejecting bandwidth requests smaller than the bad “max_tx_burst” CoS parameter.

Workaround: Ensure that the TFTP configuration file for the modem has all the five class of service configuration parameters set to avoid CMTS from using uninitialized CoS parameters.

Fix: This problem has been fixed by making the CMTS use default CoS parameter values when the corresponding parameters are not received in the CoS configuration TLV (Type Length Value) block of the registration request message.

- CSCdk04428
IPX fast switching does not work over an ISL link.
There is no known workaround.
- CSCdk04503
Trying to run Voice over IP (VoIP) traffic correctly over an encrypted IP link causes the router to reload. This only happens with VoIP traffic, and it only happens when encryption is configured. Encrypting non-VoIP traffic works correctly, and running VoIP traffic over an unencrypted link works correctly.
There is no workaround.
- CSCdk07698
The SID (Service ID) of the modem that fails to register with the CMTS (Cable Modem Termination System) is immediately assigned to another newly signed-on modem. This causes both of the modems to use the same SID to communicate with the CMTS.
Workaround: Make sure all the modems are properly registered.
Fix: Delay using the SID of the failed registered modem to assign to the newly signed-on modem.
- CSCdk08441
On Cisco 2600 series routers running Release 11.3(2)XA1 or Release 11.3(3a)T, WIC-1B-U modules might not be recognized during the start-up process. If this problem occurs, the affected WICs must be returned for replacement.
Workaround: Upgrade the router to Release 11.3(3a)T1 or later.
- CSCdk09450
On Cisco 2600 series routers running Cisco IOS Release 11.3(2)XA1 or Release 11.3(3a)T, and configured with 20 MB of RAM, the router fails to complete the start-up sequence.
Workaround: Configure the router with 24 MB or 16 MB of memory. Upgrade to Cisco IOS Release 11.3(3a)T1 or later.
- CSCdk16111
The **full-duplex** interface command does not configure FE interfaces to full-duplex mode. This affects only the FE interface on the Cisco 3600 series FE2P network module.
There is no workaround.

Wide-Area Networking

- CSCdj89726
MS clients that connect and request callback do not get a callback from the Cisco access server. The incoming interface on the access server is some form of dialer. A log “debug dialer” includes a message of the form “callback to user-joe already pending (legacy).”
There is no known workaround.
- CSCdj93549
A Cisco 3640 running Release 11.3(2)T is sending a DISCONNECT on a PROGRESS indication (value 0x8288 = In-band info or appropriate now available) from the switch.
There is no workaround.

- CSCdk18271

When running Release 11.3(4)T, the configuration command **frame-relay interface-dlci** is not working. This affects Frame Relay users who need to configure point-to-point subinterfaces on Cisco 100x, Cisco 160x, Cisco 2600, and Cisco AS5200 platforms.

There is no known workaround.

Resolved Caveats—Release 11.3(3)T

All the caveats in this section are resolved in Release 11.3(3)T. This section describes only severity 1 and 2 caveats.

Access Server

- CSCdj73991

If the T1 controller framing mode changes after a **cas-group** is configured, the state of the a/b/c/d bits can become unreliable. This is only known to be a problem under heavy load. The symptom is a high percentage of connection failures.

Workaround: Remove and then reenter the **cas-group** commands on the controllers.

- CSCdj80557

The default value of FastEthernet buffers for the Cisco AS5300 is too small. This can affect (decrease) routing performance, by causing an excessive amount of FastEthernet interface throttles.

Workaround: Increase the number of FastEthernet buffers:

```
c5300(config)# buffers fastEthernet 0 permanent 256
```

Basic System Services

- CSCdj74094

There is a problem with weighted fair queuing (WFQ) and weighted random early detection (WRED), where packets are not classified to the correct conversation or precedence. The problem occurs only for IP NetFlow and optimum switching, and only on the Cisco 7200 series platform.

Workaround: Disable optimum switching and enable NetFlow Switching.

DECnet

- CSCdj69585

When a dial-up line's idle timer expires, the line is shut down. Incoming packets are then returned to sender (if the request return flag is set) until the reenable timer has expired. This leads to misleading ping messages because they are indistinguishable from packets for targets that are unreachable.

There is no known workaround.

Interfaces and Bridging

- CSCdj90253

VIP/PA-4R and VIP/PA-4R-FDX Token Ring interfaces configured for source-route bridging (SRB) automatic spanning tree can begin cycling endlessly between “up” and “initializing” states.

Workaround: Configure manual SRB spanning tree.

- CSCdj93847

The random MAC address generation for the Bridge-Group Virtual Interface (BVI) interface does not set up an expected address because of a problem in the BVI-specific code. This problem only affects the second BVI interface creation, and the first and second BVI MAC address need to be generated by using the random MAC address generation scheme. To prevent this from happening, set up the MAC address manually immediately after the BVI interface is created.

The current code generating the MAC address for the BVI is not unique. When a second BVI interface MAC address is generated, it attempts to make sure the address is unique in the system. Somehow, the first BVI MAC address gets the same value as the second one. This causes an infinite loop to generate the unique value. Eventually, the watchdog timer process forces the system to reload.

This problem was introduced by the STP modularity commit in Release 11.3T and later.

There is no known workaround.

Miscellaneous

- CSCdj73443

Support was included to increase the switching speed of packets that were between 600 and 1524 bytes in size. This was done by locating a pool of contiguous large buffers in SRAM, such that when particles needed to be coalesced they were coalesced in SRAM only.

Unfortunately, when a buffer was allocated from this pool, the input queue count was not incremented, resulting in an interface dropping incoming packets because the input queue count was huge.

This caveat fixes the problem by removing the code that created a large SRAM contiguous buffer pool.

There is no known workaround.

- CSCdj80643

A 6-modem MICA SIMM must be installed in Bank 0 of the Digital Modem Network Module. If it is not installed, the Cisco 3640 router reloads during bootup.

There is no known workaround.

- CSCdj82169

Boardware on a Cisco AS5300 is found to slice the data incorrectly. The problem occurs at random on a per-line basis across all boards and ports running Release 11.2(10a)P1 with 2.0.1.7 portware, 1.3.3.5 boardware, rev A0 on the Amazon board. Trashed data in/out of a bad line is seen.

Workaround: Power cycle the Cisco AS5300.

If you are running PPP over the modem link, a symptom is input errors. If you are running a dialin exec session, the characters entered might be echoed out of order. If you are running a reverse Telnet session, lines of data sent from the modem to the Telnet session might appear out of order.

- CSCdj89527

In Release 11.3(2)XA, the FEC code word length is programmed improperly both in the UCD (Upstream Channel Descriptor) message and in the upstream receiver chip. This causes the system not to be Data-over-Cable Service Interface Specifications (DOCSIS) compliant. Therefore, the chip programming as well as the UCD message has been changed.

This change had to be implemented in both cable modem and Cisco uBR7200 software.

The change causes the system to be interoperable with cable modems not implementing this change, if FEC (forward error correction) and the interface configuration command **cable upstream 0 fec** is active.

A hidden CLI configuration command has been added to return the Cisco uBR7200 code to the old (non compliant) value. This command is **[no] cable compliant reed-solomon**. The default configuration setting is **cable compliant reed-solomon**.

There is no known workaround.

- CSCdj91373

Having a different IP address offered to a cable modem or its associated hosts after a DHCP release is now supported.

The client gets an IP address as long as the DHCP-server supplied address is the same each time. However, a problem occurs if the server issues another address associated with the same PC MAC address, because the previous address was released. The PC fails to get the second address because the Cisco uBR7200 series console modem attempts to ARP for the SID (Service ID) of the modem that has the PC attached to it. It fails because the DHCP reply never gets there and the CMTS (Cable Modem Termination System) does not forward the reply. Therefore, the PC's IP address never gets set.

Workaround: Enter the following configuration commands:

```
conf term
int cable X/0
no cable resolve-sid
end
```

- CSCdj91870

Updated cable modem code in conjunction with upstream problem detection code causes the system to fail after the **clear interface** command is entered on the cable interface in the Cisco uBR7200 series console modem, or if there is a glitch in the downstream direction.

The problem can be reproduced as follows:

- Use a Cisco cable modem image built at or after March 22.
- Connect the system. Wait until the modems are up. Make sure modem power level is relatively high, such as 50 dBmV.
- Issue the **clear interface** command on the uBR cable interface.
- The Cisco uBR starts to issue interface resets, thinking the US channel chip would have a problem. Also, frequency jumps might happen if spectrum management is configured.

There is no workaround.

Fix: To allow sufficient time for cable modems to complete initial ranging after a reset, the timeout after a reset is extended to 2 minutes.

- CSCdj93233

When a modem is shut down through the software, it can cause other modems to fail ranging. This is because vendor cable modem hardware still responds to ranging requests even if the cable modems are in software shutdown.

There is no known workaround.

- CSCdj95374

Modem calls attempted through CAS using more than 12 digits cause a bus error exception. This does not affect any operation of the router if the dialed digits are fewer than 13.

There is no known workaround.

- CSCdk00113

In Release 11.3(2.4)T a problem was introduced that prevents the Cisco 3600 series router from downloading the 56K MICA portware (c3600-mica-portware.2.2.3.0.bin) at bootup time. The end result is that the Cisco 3600 series router reverts back to the built-in MICA portware (version 2.0.1.7) and ignores the 2.2.3.0 version on Flash memory. This affects Cisco 3640 routers with digital modems that are trying to use the recently released c3600-mica-portware.2.2.3.0.bin file.

There is no workaround.

Resolved Caveats—Release 11.3(2)T

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

Access Server

- CSCdj77836

A Cisco AS5200 might reload with a bus error if no modem modules are installed.

There is no known workaround.

- CSCdj78344

The Cisco AS5300 might answer an inbound R2 call too quickly causing the call to terminate before it can complete training.

There is no known workaround.

Basic System Services

- CSCdj69967

The router might reload when disabling IP routing or removing the configuration for routing protocols.

There is no known workaround.

ISO CLNS

- CSCdj65166

Changes made to the IOS software that allowed a configurable number of maximum area addresses did not include a default value if none was specified. As long as both sides of the link has Connectionless Network Services (CLNS) enabled, the router reloads.

There is no known workaround.

Wide-Area Networking

- CSCdj66559

The router reloads when the static map for an active SVC is updated or deleted. With the old ATM CLI, the reload occurs when a map-group or map-list is updated or deleted while the SVC is active. With the new WAN CLI, the reload occurs when the **protocol** command in VC mode is updated or deleted while the SVC is active.

There is no known workaround.

- CSCdj71255

Spurious memory access occurs when a PVC is configured with broadcast enabled using the old ATM CLI **atm pvc** command. If **service alignment detect** is enabled, the router does not reload and continues to run.

There is no known workaround.

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.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, 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, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0403R)

Copyright © 1999–2004, Cisco Systems, Inc.
All rights reserved. Printed in USA.