



Text Part Number: 78-6018-06 Rev. E0

Caveats for Cisco IOS Release 12.0 T

July 30, 2003

This document lists severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.0 T, up to and including Cisco IOS Release 12.0(7)T3. 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 12.0 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 50.

How to Use This Document

This document describes open and resolved severity 1 and 2 caveats and select severity 3 caveats:

- The "Open Caveats" 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 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

Cisco IOS software documentation can be found on the web through Cisco.com and on the latest Documentation CD-ROM. For information on CCO, see the "Cisco Connection Online" section on page 49. For more information on the CD-ROM, see the "Documentation CD ROM" section on page 50.

Corporate Headquarters

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

Copyright © 1998-2000
Cisco Systems, Inc.
All rights reserved.

For more information on caveats and features in Cisco IOS Release 12.0 T, see the following sources:

- *Dictionary of Internetworking Terms and Acronyms*—The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this caveats document.
- *Bug Toolkit*—If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Service & Support: Software Center: Cisco IOS Software: BUG TOOLKIT**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.
- *Caveats for Cisco IOS Release 12.0*—The Caveats for Cisco IOS Release 12.0 document lists severity 1 and 2 caveats for Cisco IOS Release 12.0, up to and including Release 12.0(22). All caveats in Cisco IOS Release 12.0 are also in Cisco IOS Release 12.0 T.
- *Release Notes for Cisco IOS Release 12.0*—These release notes describe new features and significant software components for Cisco IOS software Release 12.0. All features in Cisco IOS Release 12.0 are also in Cisco IOS Release 12.0 T.
- *Cisco IOS Release 12.0 T platform-specific release notes*—These release notes describe new features and significant software components for Cisco IOS Release 12.0 T.
- *What's Hot for IOS Releases: Cisco IOS 12.0*—*What's Hot for IOS Releases: Cisco IOS 12.0* provides information about caveats that are related to deferred software images for Cisco IOS Release 12.0. If you have an account on Cisco.com, you can access *What's Hot for IOS Releases: Cisco IOS 12.0* at <http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml> or by logging in and selecting **Software Center: Cisco IOS Software: What's Hot for IOS Releases: Cisco IOS 12.0**.
- *What's New for IOS*—*What's New for IOS* lists recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. If you have an account on Cisco.com, you can access *What's New for IOS* at <http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml> or by logging in and selecting **Software Center: Cisco IOS Software: What's New for IOS**.

Note Release notes are only modified on an as-needed basis. 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, or related documents.

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

Release Notes	Cisco IOS Release	Revision Date
<i>Release Notes for Cisco IOS Release 12.0</i>	Release 12.0(8)	December 13, 1999
<i>Release Notes for Cisco uBR904 Cable Modem for Cisco IOS Release 12.0 T</i>	Release 12.0(7)T	December 13, 1999
<i>Release Notes for Cisco uBR924 Cable Modem for Cisco IOS Release 12.0 T</i>	Release 12.0(7)T	December 13, 1999
<i>Release Notes for the Cisco 1000 Series Routers for Cisco IOS Release 12.0 T</i>	Release 12.0(7)T	December 13, 1999
<i>Release Notes for the Cisco 1400 Series Routers for Cisco IOS Release 12.0 T</i>	Release 12.0(7)T	December 13, 1999

Release Notes	Cisco IOS Release	Revision Date
<i>Release Notes for the Cisco 1600 Series Routers for Cisco IOS Release 12.0 T</i>	Release 12.0(7)T	December 13, 1999
<i>Release Notes for the Cisco 1700 Series Routers for Cisco IOS Release 12.0 T</i>	Release 12.0(7)T	December 13, 1999
<i>Release Notes for the Cisco 2500 Series Routers for Cisco IOS Release 12.0 T</i>	Release 12.0(7)T	December 13, 1999
<i>Release Notes for Cisco 2600 Series for Cisco IOS Release 12.0 T</i>	Release 12.0(7)T	December 13, 1999
<i>Release Notes for Cisco 3600 Series for Cisco IOS Release 12.0 T</i>	Release 12.0(7)T	December 13, 1999
<i>Release Notes for Cisco MC3810 for Cisco IOS Release 12.0 T</i>	Release 12.0(7)T	December 13, 1999
<i>Release Notes for Cisco 4000 Series for Cisco IOS Release 12.0 T</i>	Release 12.0(7)T	December 13, 1999
<i>Release Notes for Cisco AS5200 Universal Access Servers for Cisco IOS Release 12.0 T</i>	Release 12.0(7)T	December 13, 1999
<i>Release Notes for Cisco AS5300 for Cisco IOS Release 12.0 T</i>	Release 12.0(7)T	December 13, 1999
<i>Release Notes for Cisco AS5800 Universal Access Servers for Cisco IOS Release 12.0 T</i>	Release 12.0(7)T	December 13, 1999
<i>Release Notes for Cisco 7000 Family for Cisco IOS Release 12.0 T</i>	Release 12.0(7)T	December 13, 1999
<i>Release Notes for Cisco uBR7200 Series for Cisco IOS Release 12.0 T</i>	Release 12.0(7)T	December 13, 1999

Last Maintenance Release of Cisco IOS Release 12.0 T

Cisco IOS Release 12.0(6)T has been renamed 12.0(7)T to align this release with the 12.0(7) mainline release. The closed caveats for Release 12.0(7)T are identical to the caveats closed in the 12.0(7) mainline release. There was no change in the feature content of the renamed release--the features in 12.0(6)T are the same as 12.0(7)T. Release 12.0(7)T is the last maintenance release of the 12.0 T release train.

Customers needing closure of caveats for the 12.0 T features should migrate to the 12.1 mainline release, which has the complete feature content of Release 12.0 T and will eventually reach General Deployment (GD). Release 12.0 T is a super set of the 12.0 mainline release, so all caveats closed in the 12.0 mainline are also closed in 12.0 T.

Resolved Caveats—Cisco IOS Release 12.0(7)T3

Cisco IOS Release 12.0(7)T3 is a rebuild release for Cisco IOS Release 12.0(7)T. The caveats in this section are resolved in Cisco IOS Release 12.0(7)T3 but may be open in previous Cisco IOS releases.

- CSCeb40433

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—Cisco IOS Release 12.0(7)T2

Cisco IOS Release 12.0(7)T2 is a rebuild of Cisco IOS Release 12.0(7)T. All caveats in this section have been resolved in Cisco IOS Release 12.0(7)T2 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>

Open Caveats—Cisco IOS Release 12.0(7)T

This section describes possibly unexpected behavior by Cisco IOS Release 12.0(7)T. All the caveats listed in this section are open in Cisco IOS Release 12.0(7)T. This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCdm52201

A PA-A1 port adapter might exhibit aborts and input errors for packet sizes over 1500 bytes when used in a Cisco 7200 VXR series router with an NPE-300. There is no workaround.

- CSCdm70663

A Cisco 7500 router that is running Cisco IOS Release 12.0 T and has a Versatile Interface Processor (VIP) might reload if you enter the **show line** command while several Telnet and if-con sessions are running concurrently. This condition occurs because using if-con to get information from the VIP is unsupported.

Workaround: Obtain statistics from a VIP using the **show controllers vip slot# command** command.

- CSCdp03448

When ISDN calls are brought up on a Cisco router that has ISDN traps configured, memory leaks will occur in the Simple Network Management Protocol (SNMP) trap process. In addition, some ISDN traps will be lost because of the invalid variable bindings (varBinds) that cause the leaks.

Workaround: Remove all **snmp-server enable traps [isdn]** global configuration commands from the router.

- CSCdp21693

A Route Switch Processor (RSP4) that is running Cisco IOS Release 12.0(5)T1 might experience intermittent interprocess communication (IPC) problems that causes the Forwarding Information Base (FIB) to disable the linecards involved. There is no workaround.

- CSCdp26307

A Cisco 7206VXR router with a network processing engine (NPE)-300 that is configured for source bridging together with a Token Ring-Inter-Switch Link (TR-ISL) might constantly reload with the following error message:

```
Rebooted by watchdog hard reset
```

There is no workaround.
- CSCdp27051

If you enable IP route-caching (IP fast-switching) on a PPP serial interface that is part of a multilink bundle, traffic that is destined for that bundle might stop.

Workaround: Shut down the serial interfaces before entering the **ip route-cache** command, and then enable the interfaces.
- CSCdp28587

When you configure a named EXEC authorization method list, the default network authorization method list will be erased from the configuration.

Workaround: Reconfigure the default network authorization method list.
- CSCdp38982

When Label Switch Router (LSR)-A is transmitting Multiprotocol Label Switching (MPLS) encapsulated IP frames to LSR-B, and LSR-B is removing the last label and transmitting the resulting IP frame onto an Idle Line State (ILS) link, IP packets less than 44 bytes will be received as cyclic redundancy check (CRC) errors. There is no workaround.
- CSCdp42381

If you are using IOS Firewall, **ip http authentication {aaa}** might disappear from the router configuration. There is no workaround.
- CSCdp43912

After you add several interfaces to a Cisco 7206VXR router that is running Cisco IOS Release 12.0(4)T or Cisco IOS Release 12.0(5)T1, you will be able to see them in the router configuration, but a Simple Network Management Protocol (SNMP) walk (ifEntry) does not show all the interfaces.

Workaround: Reload the router. The MIB table will be reordered, and all of the interfaces will be available in the configuration and through a SNMP walk.

IBM Connectivity

- CSCdm78005

A Cisco 4500 router might experience memory alignment errors in Advanced Peer-to-Peer Networking (APPN). There is no workaround.

Interfaces and Bridging

- CSCdm08671

Packet-over-SONET (POS) port adapter interfaces on a network processing engine (NPE)-300 do not achieve line rate with 512 bytes and above because of output drops. There is no workaround.

- CSCdm56161

A High-Speed Serial Interface (HSSI) port adapter is disabled with following error message if the load reaches approximately 40 Mbps:

```
Jun 23 09:43:23 vgs18 20: .Jun 23 09:43:19: %MUESLIX-1-STOPFAIL: Mx serial,
Hssi2/0 Stop Failed at disable port Jun 23 09:43:23 vgs18 22: .Jun 23 09:43:19:
%MUESLIX-1-STOPFAIL: Mx serial, Hssi2/0 Stop Failed at disable port
```

There is no workaround.

- CSCdm75730

If you configure Gigabit Ethernet with IEEE 802.1Q for virtual LAN (VLAN) application, traffic might not be able to pass through the interface. There is no workaround.

- CSCdm76205

A Cisco router using Multiprotocol Label Switching (MPLS) tunneling over serial lines might reload with the following error message:

```
gdb_crash_restore+0x30] exception_write_core+0x18] vip_pak_to_host+0x858]
serial_process_receive_packet_check_ip+0x83c] mxt_rx_interrupt+0x508]
mxt_interrupt_handler+0x1d8] mxt_8t_interrupt_wrapper+0x18]
```

There is no workaround.

- CSCdp08975

A Cisco 7200 router that is configured for RFC1577 and is not acting as an Address Resolution Protocol (ARP) server might experience a condition where the status of ATM VCs change in spite of the traffic flowing on them. This condition occurs if RFC1577 is configured on the main interface.

Workaround: Configure RFC1577 on a subinterface.

- CSCdp15196

A Cisco 7507 router that is running Cisco IOS Release 12.0(4)T might not return the correct results if there is a change in the hold-queue value in any of the serial interfaces of a PA-8T port adapter in a VIP2 motherboard. Although the size of the output queue seems to change after you enter the **hold-queue out** interface configuration command, there is no real change. There is no workaround.

- CSCdp20709

The address that is assigned by Dynamic Host Configuration Protocol (DHCP) might not be accepted if the remote client that is terminating a PPP session into your virtual template has tried to use a different address. There is no workaround.

- CSCdp35902

On a Cisco 7500 series router that is running Cisco IOS Release 12.0(4)T, Fast Ethernet might append extra bytes in Ethernet frames. There is no workaround.

- CSCdp37455

A Cisco AS5800 universal access server with E1 PR1 lines that is running Cisco IOS Release 12.0(4)XJ2 or Cisco IOS Release 12.0(5)T1 might drop Serial Line Internet Protocol (SLIP) connections after Cisco IOS installs a route for a remote user. PPP users (both asynchronous and ISDN) can connect, but the SLIP users cannot connect with MICA modems that are running 2620 portware. There is no workaround.

- CSCdp41810

A Cisco 7500 series router with a VIP2-based Fast Ethernet port adapter might exhibit the following message:

```
%CBUS-3-CCBPTIMEOUT: CCB handover timed out, CCB 0x5800FFB0, slot 9 -Traceback=
60338B60 603362B8 603368D8 60310404 60335C28 6023418C 602B6AFC 602B6 AE8
```

Workaround: Enter the **no cdp run** global configuration command to disable Cisco Discovery Protocol (CDP).

IP Routing Protocols

- CSCdm19562

A Cisco router that is running Cisco IOS Release 12.0(3)T might reload with a bus error in OSPF while OSPF is trying to delete an external path. There is no workaround.

- CSCdm47603

If h323 is configured on a remote interface of a router that is configured as a standby gatekeeper, the local interface Enhanced Interior Gateway Routing Protocol (IGRP) might not advertise a route to the remote network. If the standby gatekeeper router in this situation is a Hot Standby Router Protocol (HSRP) router that takes over for the HSRP active router, the other routers on the local network will lose their route to the remote network.

Workaround: Configure a static route to the remote network with the HSRP virtual address as the next hop.

- CSCdp08764

When traffic is flowing across a multilink bundle, there might be a noticeable pause in throughput when a B channel is added or removed from the bundle. There is no workaround.

- CSCdp15119

A Cisco router might reload when Resource Reservation Protocol (RSVP) is configured on an interface but not on the subinterfaces, and weighted fair queueing (WFQ) is enabled. There is no workaround.

- CSCdp15580

A Cisco router that is running Cisco IOS Release 12.0 T and is configured with the **aggregate-address [as-set]** router configuration command might not provide complete information in the AS_PATH. There is no workaround.

- CSCdp28188

Border Gateway Protocol (BGP) peering might fail because of invalid or corrupt autonomous system path attributes that are sent in the BGP updates. There is no workaround.

ISO CLNS

- CSCdp32259

If you configure IP redistribution into the Intermediate System-to-Intermediate System (ISIS) protocol and configure the level or metric type to be something other than the default, that information is not included when the configuration is generated with the **show running-config** command or the **show startup-config** command. This situation only occurs if you are running Cisco IOS Release 12.0 T.

Workaround: Reconfigure the level or metric type after each reboot.

- CSCdp42588

When two events occur within a short period of time that cause a Cisco router that is running Intermediate System-to-Intermediate System (IS-IS) to regenerate a new link-state packet (LSP), a race condition might occur that can cause the router to skip the second LSP generation. This situation results in the router not advertising its current state to the rest of the network. (For example, an adjacency might be missing from its LSP, or an old adjacency that does not exist anymore is still advertised.) All the routers in the network will then compute invalid IP routes.

This condition occurs only in Cisco IOS Release 12.0(5)T and later releases, and can only occur when IS-IS is configured for IP routing. If a router runs IS-IS in Connectionless Network Service (CLNS) only, this condition will not occur. If a router has only a few IP routes in the IP routing table, this situation is less likely to occur than if there are many IP routes in the IP routing table.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on any interface that is configured for IS-IS.

Miscellaneous

- CSCdk51439

If flow-acceleration is enabled, then disabled, and encryption is subsequently enabled, the router may unexpectedly reload.

Workaround: Avoid enabling and then disabling flow-acceleration.

- CSCdk88739

If you run a hub and spoke Frame Relay configuration, and the hub router is set to be a multipoint interface, Dynamic Host Configuration Protocol (DHCP) requests will fail.

Workaround: Configure both the hub and spoke to use point-to-point subinterfaces. Another workaround is to configure the DHCP server address on the spoke router instead of specifying the network address on which the DHCP server resides. This DHCP server address turns into a unicast address instead of a directed broadcast, which happens in the current scenario.

- CSCdm17319

The RADIUS Call Filter Attribute (attribute 243) does not work properly. Instead of operating as an interesting traffic filter, it is operating as a data filter like attribute 242. There is no workaround.

- CSCdm24965

The D-channel interface gets reenabled automatically after it is shut.

Workaround: Shut the controller instead of the D-channel interface.

- CCSCdm26423

Changing your portware version from the default to another bundle or changing it back again during boot up or operation might cause modems to be marked in “D” state if certain messaging failures occur between the router shelf and the dial shelf. This situation is very likely to occur when a portware download is initiated and then followed by the **clear modem** command.

Workaround: Wait until all downloads are complete before entering the **clear modem** command.

- CSCdm30178

A Cisco router might reload with a bus error while you are switching encapsulation between High-Level Data Link Control (HDLC) and Frame Relay on an interface that has been configured with the **ip rtp header-compression** interface configuration command without the **ip tcp header-compression** interface configuration command.

Workaround: Enter the **ip tcp header-compression** command before switching encapsulation.
- CSCdm31924

A Cisco AS5800 series access server that is configured for loopstart might not respond to ABCD bits being sent to the router if the T3 circuit goes down.

Workaround: Change the signalling (sas-loopstart, groundstart, and so on) and then go back to loopstart.
- CSCdm40757

If you are running data and voice together on the same WAN interface on a Cisco MC3810 multiservice access concentrator, you might configure the data fragmentation in a way that causes a large amount of delay jitter for voice packets. In this situation, the DSP might not adequately adapt its dejitter playout process, which leads to a degradation in voice quality.

Workaround: Increase the playout-delay nominal setting in the voice-port configuration. For example, enter the **playout-delay {nominal} 120** voice-port configuration command.
- CSCdm42284

A Cisco 1720 router might reload if you use IP Security (IPSec) with Checkpoint FW1 version 4.0. This condition occurs with Cisco 1720 routers with 48 MB of memory running the Cisco IOS Release 12.0(4)T IP/FW PLUS IPSEC 56 image. There is no workaround.
- CSCdm45861

Cisco express forwarding (CEF) does not function properly on a router that is performing decryption. The other router functions are not affected. There is no workaround.
- CSCdm48920

If you are disabling Protocol Independent Multicast (PIM) on a Cisco AS5800 universal access server that is running Cisco IOS Release 11.3(9)AA, the router will reload.

Workaround: Avoid reconfiguring the router during production hours and periods of high traffic.
- CSCdm52748

Low-end platforms will experience spurious accesses (or reload in the case of Cisco 1700 series routers) if you disable Cisco express forwarding (CEF) on a serial interface by entering the **no ip route-cache cef** command, then change the encapsulation of that interface and then reenable CEF on the serial interface by entering the **ip route-cache cef** command.

Workaround: Disable CEF.
- CSCdm56454

If you have a large configuration file (for example, where a large number of permanent virtual circuits (PVCs) configured for PPP over ATM), the node route processor (NRP) might take as long as 10 to 30 minutes to complete bootup. This situation occurs because the NRP must read the configuration files and build up the PVCs.

Workaround: Design a smaller configuration file.

- CSCdm57759
A Cisco 7200 series router with an 8-port channelized E1 card running Cisco IOS Release 12.0(4)T might experience a memory leak in the small buffer pool.
Workaround: Monitor the input/output (I/O) memory and reload the router when it is too low.
- CSCdm59751
A Cisco 7500 series router might drop encrypted packets if those packets are routed over a Token Ring port adapter. There is no workaround.
- CSCdm69594
The interface delay metric is set incorrectly for port channel interfaces where one or more Gigabit Ethernet interfaces are grouped into a channel. The delay for a single Gigabit Ethernet interface is 10 microseconds. The delay for a port channel made up of one or more Gigabit Ethernets is 100 microseconds. The incorrect setting might seriously impact routing protocols that use interface delay as part of the metric (for example, Enhanced Interior Gateway Routing Protocol (EIGRP)), and might cause the routing protocol to take a route through a single interface over a route through a port channel.
Workaround: Manually configure an appropriate delay under the port channel interface by entering the **delay** *tens of microseconds* interface configuration command.
- CSCdm72571
A Cisco router might reload if it is using STAC compression over PPP with fancy queueing.
Workaround: Use first-in-first-out (FIFO) queueing.
- CSCdm78679
A Cisco 1720 router that is running Cisco IOS Release 12.0(5)T might reload with the following error message if you shut down a serial interface while packets are being routed to a dialer interface:

```
System returned to ROM by error - a SegV exception, PC 0x802Ac04C
```


There is no workaround.
- CSCdm81194
In a Channel Associated Signalling (CAS) environment, a DS0 might become unavailable if the line is seized for an outgoing call and there is no response from the remote end. In this situation, the Cisco AS5300 access server is configured to establish the maximum number of outgoing calls possible for the number of DS0s in the system. Each unavailable DS0 will result in the following message:

```
no ds0 available for modem
```


There is no workaround.
- CSCdm82271
If you attempt to clear all active calls associated with an ISDN D-channel on a Cisco AS5800 by entering the **clear interface serial** *shelf/slot/port:D_Channel_Timeslot* EXEC command, the calls are not terminated.
Workaround: Clear one call at a time by entering the **clear interface** *shelf/slot/port:B_Channel_Timeslot* EXEC command.
- CSCdm86201
Under rare conditions, Cisco routers that are running Cisco IOS Release 12.0 T might reload if you reconfigure a crypto map while the crypto map is being used. There is no workaround.

- CSCdm87515

A Cisco router that is running IP Security (IPSec) might reload if you enter the **clear crypto sa** command while the router CPU utilization is near 100 percent because of high IPSec traffic rates. There is no workaround.
- CSCdm90336

A switch/network access server might get out of sync due to IDLE being sent by the network access server to the switch prior to being ready to accept the next call. When the call comes in, the switch no longer sends calls to this particular DS0 until the network access server sends IDLE back to switch. There is no workaround.
- CSCdm91466

The Cisco Resource Pool Manager (RPM) might hold memory and not release it, which causes the router to run out of memory and pause indefinitely. There is no workaround.
- CSCdm93596

Although call success ratio (CSR) tests on a Cisco AS5300 with E1R2 signalling might be greater than 99 percent, one or more DSPs might fail after several hours (usually from 5 to 20 hours), and calls cannot be made through the failed DSPs. This situation occurs under a load of 60 calls within a 30-second period. Calls can still be made through other DSPs in the DSP pool.

Workaround: Upgrade from 542 DSP modules to 549 DSP modules.
- CSCdm95317

Statistics for per ATM PVC Weighted Random Early Detection (WRED) are not passed from a Versatile Interface Processor (VIP) to a Route Switch Processor (RSP). This situation gives the impression that the feature is not functioning, but the feature is functioning on the VIP. The statistics are not available to the RSP, and they cannot be displayed in the show output. There is no workaround.
- CSCdp02332

Under rare circumstances, a store-and-forward fax Simple Mail Transfer Protocol (SMTP) server might return the following message to the SMTP client even though the fax was delivered successfully:

```
450 4.4.2 Fax protocol delivery error
```

There is no workaround.
- CSCdp04045

After reloading a Cisco 2600 series router, a “memory-size iomem 6” router statement is automatically generated. If the router is reloaded using this memory size, the SS7 session will not come up.

Workaround: Enter the **memory-size iomem 40** command. This command changes the percentage of DRAM that is allocated to I/O memory, and entering this command in this situation should allow the SS7 session to come up.
- CSCdp05107

Permanent virtual circuits (PVCs) might not transmit if the configuration for the PVC is changed while the outbound rate on that PVC exceeds sustainable cell rate (SCR).

Workaround: Enter the **clear interface ATM slot/port EXEC** command when this situation occurs.

- CSCdp06175
If you configure asynchronous and synchronous connections on the same NM-4A/S or NM-81/S cards, asynchronous connectivity might be affected.
Workaround: Configure the card exclusively for asynchronous connection.
- CSCdp08454
When performing a traceroute across a Multiprotocol Label Switching (MPLS) region, the first router that label switches a packet (that is, the router following the label imposition point) will not appear. There is no workaround.
- CSCdp08621
Fax relay over IP between two Cisco AS5300 universal access servers might fail if there is a large round-trip delay, packet loss, or jitter. There is no workaround.
- CSCdp10455
A Cisco AS5800 universal access server that is running Cisco IOS Release 12.0(5)T or Cisco IOS Release 12.0(4)XJ2 might experience CPU performance problems. There is no workaround.
- CSCdp12095
Inter-Switch Link (ISL) does not work in Cisco 7100 series routers prior to the Cisco IOS Release 12.0(05)XE. There is no workaround.
- CSCdp12931
When the output-rate limit is configured on an ATM subinterface on a Cisco 7500 series router, the Distributed Committed Access Rate (DCAR) might not function properly, and impossibly high values in the “last packet” field might occur. There is no workaround.
- CSCdp13085
After 11 hours of continuous calls, the gateway tends to lose its registration with the gatekeeper, gets stuck in a loop, and cannot be brought down because there are calls in the system yet to be cleared. No other Registration, Admission, and Status (RAS) protocol transactions can occur. There is no workaround.
- CSCdp13468
If there is a large network delay for Voice over IP (VoIP) calls on a Cisco AS5300 universal access server that is running Cisco IOS Release 12.0(6)T or later releases, DSP might go into voice mode (where an audio path opens) approximately 1 or 2 seconds after the call connects.
Workaround: Enter the **no ip tcp delayed-ack** global configuration command.
- CSCdp17155
IP Security (IPSec) might cause a memory leak on a Cisco router that is running Cisco IOS Release 12.0(5.5)T if the configuration is using a dialer interface where **ip address negotiated** is enabled. There is no workaround.
- CSCdp17903
If you are configuring **virtual-profile if-needed** on a Cisco AS5200, Cisco AS5300, or Cisco AS5800 access server that is running Cisco IOS Release 12.0(7.3)T, pings and IP packets fail because of reported encapsulation failures on the dialer or serial interface. This situation does not occur if **virtual-profile if-needed** is not configured, but the router performance is affected if **virtual-profile if-needed** is not configured. There is no workaround.

- CSCdp18673

The slot order of physical cards might cause a Cisco 5200 series router to pause indefinitely. This situation occurs with the following slot order:

- slot 2: Microcom 56K card
- slot 1: MICA modem card
- slot 0: Dual E1/PRI card

Workaround: Use any other slot order configuration.

- CSCdp18789

A Cisco 2600 series router might reload when given the **physical-layer async** command while configuring for Asynchronous Security Protocols (ASP) over Block Serial Tunneling (BSTUN) when the hardware chip is a PowerQuicc chip. There is no workaround.

- CSCdp19180

Load balancing might fail on two Cisco routers that are connected to each other by three E1 links that are using multichannel port adapters. Two of the links show normal throughput, but the third has very low throughput. There is no workaround.

- CSCdp19564

A network access server might reload if there is a slow authentication, authorization, and accounting (AAA) server, and if a caller disconnection occurred right after L2F tunnel establishment but before the session establishment. There is no workaround.

- CSCdp20758

If you configure more than 300 static routes across several VPN routing/forwarding instances (VRFs) with duplicate addresses, NVGEN might fail with the following error message:

```
----- show running-config -----
```

```
Unable to read configuration. Try again later
```

There is no workaround.

- CSCdp21039

Entering the **write core** command will cause a Cisco 800 series router to reload. There is no workaround.

- CSCdp21072

You might not be able to configure static alternate gatekeepers from the command-line interface (CLI) to a gateway when specific IP ports are required. This situation does not include Registration, Admission, and Status (RAS) protocol broadcast port 1718. The gateway will reject the second gatekeeper being configured even though the IP address of the gatekeeper is different. The gateway can only rely on the existing gatekeeper during reset and reload. If the only configurable gatekeeper is not available during this time, the gateway will not be able to provide a Voice over IP (VoIP) H323 call. There is no workaround.

- CSCdp21524

A Cisco 6400 node route processor (NRP) that is running Cisco IOS Release 12.0(3)DC might receive a malformed packet. In this situation, the NRP declares the RADIUS server dead. There is no workaround.

- CSCdp22226

When a gateway switches to an alternate gatekeeper because the current gatekeeper fails or temporarily loses contact, the router might not be able to switch over to an alternate gatekeeper again even when the original gatekeeper has come back online. This situation will occur when two gatekeepers are acting as alternate gatekeepers for each other and the gateway is configured with one primary gatekeeper. This situation can be identified by entering the **show gateway** command. If there is only one alternate gatekeeper shown under the alternate gatekeeper list, then the gateway will not switch over if the current gatekeeper fails. There is no workaround.
- CSCdp22473

Intrusion detection systems (IDS) might not detect atomic signatures if they are configured outbound on an interface.

Workaround: Configure the IDS inbound.
- CSCdp22992

A Cisco router that has been configured for point-to-point or static generic routing encapsulation (GRE) tunnel copies the type of service (ToS) field from the payload IP packet header to the outgoing delivery IP packet header. But this feature will not work for multipoint or dynamic GRE tunnels. There is no workaround.
- CSCdp23461

If you delete a modulation profile that does not have all the bursts configured (Request, Initial, Station, Short, Long), the modem might not come up after the upstream is reinitialized. There is no workaround.
- CSCdp23567

When an initiating Cisco router is configured to use IP Security (IPSec) with the **crypto cisco pregen-dh-pairs** command, the initiator will cease to operate if the connection is placed in a down state then returned to an up state by a remote peer. If this occurs, the Cisco router will appear to pause indefinitely, and you will need to restart the router.

Workaround: Enter the **no crypto pregen-dh-pairs** command.
- CSCdp24671

If you have two Cisco switches connected on Gigabit Ethernet Inter-Switch Link (ISL) trunk using SVM 1/1 and with Hot Standby Router Protocol (HSRP) configured on a Gigabit Ethernet port channel with ISL encapsulation in a Cisco switching module, then the module might reload when the HSRP group 255 becomes active. This situation can also occur with dot1q(802.1q) trunking. There is no workaround.
- CSCdp27141

A Cisco router that is configured for SNA Switching Services (SNASw) might reload in ntl_avl_next(0x60d2bf1c)+0x20. There is no workaround.
- CSCdp27202

A Cisco 7206VXR router might lose I/O memory in tunnel interfaces and hang up after operating 48 to 72 hours. The router will first lose the routing table, then lose the connections to the interfaces, and then respond to the console port. There is no workaround.
- CSCdp27441

When using Cisco Transaction Connection (CTRC), a Cisco router might reload during stress-related situations at DispatchMessage. There is no workaround.

- CSCdp28756

Box-sourced voice packets are not compressed on Cisco 2600 series routers and Cisco 3600 series routers that are using Quad Integrated Communications Controller (QUICC) serial lines. This condition occurs when a voice packet originates on a router and Rapid Transport Protocol (RTP) compression is configured on the QUICC interface over which the packet is to pass. The packet will be sent decompressed.

Workaround: Disable fast switching on the interface.

- CSCdp28859

When `cch323_call_cleanup()` is called twice on a Cisco router, the result is that the `ccb` block in the `RBTree` link list is freed. Any attempt to access the deleted `ccb` block will cause the router to reload. There is no workaround.

- CSCdp28955

If you are using a Systems Network Architecture (SNA) Switch with control flows over Rapid Transport Protocol (RTP) functionality that is not over High Performance Routing IP (HPR IP), you might encounter a deadlock where the SNA switch does not forward packets appropriately. There is no workaround.

- CSCdp31378

If you shut down an FE0 interface on a Cisco 3660 router, the router might reload with the following message:

```
%ALIGN-1-FATAL: Illegal access to a low address addr=0x14, pc=0x60B02954,
ra=0x60B02938, sp=0x62035DA8
Unexpected exception, CPU signal 10, PC = 0x60B02954
$0 : 00000000, AT : 61800000, v0 : FFFFFFFF, v1 : 000000B7 a0 : 00000000, a1 :
0000FF00, a2 : 000000B6, a3 : 000000BA t0 : 00000018, t1 : 3401FF01, t2 : 3401E100,
t3 : FFFF00FF t4 : 602C16C8, t5 : 00000000, t6 : 62035EB0, t7 : 00000163 s0 :
61EA9000, s1 : 00000010, s2 : 61EA9044, s3 : 61EA9000 s4 : 61EBC900, s5 : 00000000,
s6 : 61EA9008, s7 : 61EA9000 t8 : 0000010A, t9 : 00000000, k0 : 62083B60, k1 :
602C3668 gp : 617FFC00, sp : 62035DA8, s8 : 611F0000, ra : 60B02938 EPC : 60B02954,
ErrorEPC : BFC00CC4, SREG : 3401FF03 Cause 0000000C (Code 0x3): TLB (store)
exception
```

There is no workaround.

- CSCdp31471

The Available Bit Rate (ABR) feature on the PA-A3 port adapter is not functioning properly. The PA-A3 driver can send and receive forward resource management (FRM) cells, but cannot transmit backward resource management (BRM). There is no workaround.

- CSCdp32262

When a gatekeeper does not receive responses to its Location Requests (LRQs) from a peer gatekeeper, the first gatekeeper might become unresponsive to requests from its own clients, and no new calls are admitted. If you enable **debug ras** on the gatekeeper, you will receive the following repeated messages:

```
00:16:59:      RASLib::RASsendLRQ:LRQ (seq# 8) sent to 1.14.93.83
00:17:02:      RASLib::ras_sendto:msg length 58 from 1.14.93.92:9679 to
1.14.93.83:1719
00:17:02:      RASLib::RASsendLRQ:LRQ (seq# 8) sent to 1.14.93.83
00:17:05:      RASLib::ras_sendto:msg length 58 from 1.14.93.92:9679 to
1.14.93.83:1719
00:17:05:      RASLib::RASsendLRQ:LRQ (seq# 8) sent to 1.14.93.83
```

```
00:17:08:      RASlib::ras_sendto:msg length 58 from 1.14.93.92:9679 to
1.14.93.83:1719
```

No corresponding messages indicate that an LCF or LRJ response with the same sequence number (seq# 8 in the example) was received. Generally, when the communication path to the problem peer recovers, the situation should be resolved. However, under certain circumstances, you may need to enter the **shutdown** command followed by the **no shutdown** command on the gatekeeper. There is no workaround.

- CSCdp32993

A SNA switch link station can sometimes get stuck in “pending inact” state, and the link station is unusable until the SNA switch is restarted. There is no workaround.

- CSCdp33819

If you enter the **show users** command, you might see that the Virtual Exec process is running on the modem even when no users are connected. This situation does not affect the allocation of the modem for subsequent sessions. The next user that logs in to the modem will clear the condition. There is no workaround.

- CSCdp34696

When all B channels fill on the primary T1 of a four-member Non-Facility Associated Signalling (NFAS) group with no backup D channel, outbound modem calls might fail with the following message:

```
ERROR:EVENT_FROM_ISDN:(9D1E):DEV_CALL_PROC:vdev_common is NULL
ISDN Se0:23:CALL_ACCEPT:VOICE ERROR FC:bchan 22, call id 9D1E
```

There is no workaround.

- CSCdp35038

Versatile Interface Processors (VIPs) might reload when a 2FE port adapter is installed during bootup or configuration. There is no workaround.

- CSCdp35147

If more than 35 to 40 connections are active on the same Double-density Modem Module (DMM) modem card, and there is a large volume of unframed (non-PPP) data output on the modems, the Router Shelf Processor load might become very high, and data output to the modems may be lost. There is no workaround.

- CSCdp36462

When IOS Firewall is running on a Cisco router with Fast Ethernet subinterfaces using 802.1Q encapsulation, Context-based Access Control (CBAC) appears to run in fast switching mode, but CBAC stops inspecting traffic after an indeterminate period of time. This situation does not occur in process switching mode.

Workaround: Configure CBAC for process switching.

- CSCdp38379

In a hub and spoke model where customer edge routers (CEs) of different Virtual Private Networks (VPNs) are connected to the same provider edge router (PE), an import route that is not connected might be installed as connected. This situation results in a loss of connectivity from the other connected VPN routing/forwarding instances (VRFs) if proxy ARP is disabled on the CE. There is no workaround.

- CSCdp40032
A Cisco AS5300 series access server that is running Cisco IOS Release 12.0(4)T with VCWare 2.52 or Cisco IOS Release 12.0(5)T2 with VCWare 4.04 gets stuck in the TEI_ASSIGNED state when connected to NEC private automatic branch exchange (PABX). There is no workaround.
- CSCdp40810
A Cisco 7507 router with **ip cef** enabled on the interface might cause virtual LAN (VLAN) traffic to be dropped.
Workaround: Disable **ip cef** on global configuration, or enable **ip cef** on global configuration but disable it on the packet output interface by entering the **no ip route-cache cef** command to restore the network.
- CSCdp41625
If there is a cable modem connected to another modem card and MIB walk docsIfCmtsObjects containing docsIfCmtsCmStatusTable, the Cisco uBR7246 Universal Broadband Router might appear to pause indefinitely.
Workaround: Reload the router after performing an online insertion and removal (OIR).
- CSCdp41749
If you enter the **show cable flap-list** command while baseline privacy is active, the router will reload. There is no workaround.
- CSCdp41901
If a DLUR/DLUS connection fails, downstream LU-LU sessions might be terminated on downstream devices configured for ANS=CONTINUE, which should not normally be affected. There is no workaround.
- CSCdp42484
The **cable source-verify dhcp** command does not function properly when baseline privacy interface (BPI) is active. There is no workaround.
- CSCdp42529
A Cisco 7200VXR router might experience a situation where switched virtual circuits (SVCs) are disconnected intermittently and then recovered after 7 to 20 hours. There is no workaround.
- CSCdp42986
Sensitive customer information (such as telephone numbers) might be available at privilege level 1, which is the default for a nonenabled user.
Workaround: Configure the default privilege level to be 0 by entering the **privilege level 0** line configuration command.
- CSCdp43778
If you configure a subinterface on a Cisco 2600 series router for operation, administration, and maintenance (OAM), and the permanent virtual circuit (PVC) bounces, the PVC and the interface will not come back up unless you enter the **shutdown** command followed by the **no shutdown** command on the interface. This situation does not occur if the PVC is configured without OAM. There is no workaround.
- CSCdp44159
Encapsulation fails between a Cisco 7100 series router and a Cisco Catalyst 2900 Series XL switch, but Cisco Discovery Protocol (CDP) functions properly. There is no workaround.

- CSCdp45718
A Tag Forwarding Information Base (TFIB) table might show directly connected routes as being remote. There is no workaround.
- CSCdp45970
A Route Switch Module (RSM) might corrupt the Routing Information Field (RIF) on a Logical Link Control (LLC1) frame when running data-link switching (DLSw). There is no workaround.
- CSCdr91706
A defect in multiple releases of Cisco IOS software will cause a Cisco router or switch to halt and reload if the IOS HTTP service is enabled, browsing to [http://router-ip/anytext/?/](http://router-ip/anytext?/) is attempted, and the enable password is supplied when requested. This defect can be exploited to produce a denial of service (DoS) attack.

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

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

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

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

Novell IPX, XNS, and Apollo Domain

- CSCdm52650
Configuring IPX-EIGRP over Frame Relay links might cause memory leaks. There is no workaround.

Wide-Area Networking

- CSCdk68516
Removing a dialer interface while a call is up can result in the loss of use of one B channel.
Workaround: Reload the router to bring it back.
- CSCdm02110
A Cisco 3800 series router might receive the following error when receiving an inbound ISDN call:

```
ISDN ERROR: Module-13_sdl_u Function-Ux_BadMsg Error-Source ID = 400 Event = AB
```


There is no workaround.
- CSCdm05357
Layer 2 Tunnel Protocol (L2TP) gets stuck parsing an invalid control message with a zero-length attribute-value pair (AVP). There is no workaround.

- CSCdm12179

A multilink interface might stop processing received packets from the peer if the peer multilink interface went down and came back up. The **show ppp multilink** command will indicate “received lost fragments” when this caveat is encountered.

Workaround: Clear the multilink interface.
- CSCdm17243

Link control protocol (LCP) might fail on some Cisco routers that are running Cisco IOS Release 12.0(4)T if the maximum transmission unit (MTU) on the physical interface is less than 1500.

Workaround: Enable PPP encapsulation on the physical interface, and then set the MTU to be less than or equal to 1500.
- CSCdm23314

On a Cisco 3640 router running Cisco IOS Release 12.0(2a)T1 with MICA modems, Cisco dialout fails when a local number is called. The router returns the “not end to end isdn” call-blocked group restriction error. Any call to a long distance number succeeds. There is no workaround.
- CSCdm39954

When dialer rotary group is specified for a group-asynchronous interface, the **encapsulation ppp** command might disappear from the configuration after a reboot.

Workaround: Reenter the **encapsulation ppp** command after reboot.
- CSCdm42116

A Cisco router that is running Cisco IOS Release 12.0 T might show the following message after activating the Dialer interface when weighted fair queuing (WFQ) is enabled:

```
WFQ : Rcvd incorrectly initialized packet
```

Workaround: Disable WFQ.
- CSCdm57714

A member of a large-scale dialout stack group might continue to bid for outgoing calls even if it does not have the capability to actually make the outgoing call (T1/E1 cable is unplugged or PRI is not up, and so on).

Workaround: Manually remove the member from the stack group until the network access server (NAS) is restored to full working condition.
- CSCdm61615

The National German BRI switch type 1TR6 is not supported for voice calls. There is no workaround.
- CSCdm71990

A Cisco 3640 router might reload during a manual configuration for a dialer timeout event. This situation occurs if any connections are up while you are reconfiguring dialer parameters.

Workaround: Bring down the connections by shutting down the interface. Reconfigure the dialer parameters, and then bring the connections back up.
- CSCdm79968

When performing virtual private dialup network (VPDN) callback, the tunnel might close before Layer 2 Tunnel Protocol (L2TP) dialout takes effect. There is no workaround.

- CSCdm85397
A Cisco router might reload because of illegal access to a low memory location when there are close to 4000 active X.25 calls. There is no workaround.
- CSCdm87409
In a virtual private dialup network (VPDN) scenario, the accounting stop record shows “disc-cause=2” and “disc-cause-ext=1011” regardless of the actual reason for the disconnect (for example, password failure or Link Control Protocol (LCP) failure). There is no workaround.
- CSCdm88527
A Cisco 804 router that is running Cisco IOS Release 12.0(4)T1 or Cisco IOS Release 12.0(5)T with an IP image might not drop the existing data calls when it receives inbound analog calls. The ISDN switch type in this situation is basic-DMS-100. There is no workaround.
- CSCdm90246
A Cisco 804 router that is running Cisco IOS Release 12.0(5)T with the c800-nsy6-mw image might reload if you ping an Internet address that physically connects both B channels, and then lift the receiver on the telephone connected to the plain old telephone service (POTS) port. There is no workaround.
- CSCdm94290
Ping packets for protocols other than IP might be dropped if you configure all BRI interfaces with the **isdn fast-rollover-delay /** interface configuration command, and you are running Cisco IOS Release 12.0(6.2)T. The first several hundred ping packets pass, but then the later packets are dropped. In this situation, pings will fail even if you remove the **isdn fast-rollover-delay** from all BRI interfaces. You will need to reload the router. This situation occurs with IPX, AppleTalk, CLNS, DECnet, VINES, and XNS in legacy DDR, but does not occur in IP and bridging. There is no workaround.
- CSCdp03746
If you have TCP retransmission over an Layer 2 Forwarding (L2F) or Layer 2 Tunnel Protocol (L2TP) tunnel when the TCP host interface is Cisco express forwarding (CEF)-switching, the router might reload after the following sequence:
 - 1) You start a Telnet session from the client into the home gateway (HGW) loopback address, which is Virtual Private Network (VPN)-enabled.
 - 2) You enter the **show tech** command in the Telnet session to generate TCP data traffic from HGW to the client.
 - 3) While TCP data traffic is running from HGW to the client, you shut down the Ethernet interface on the network access server over which L2F is running, or close the PPP, which closes the L2F connection. You then bring back up the Ethernet interface or reestablish the PPP and L2F connection before the Telnet session times out.
 - 4) HGW now tries to resend the TCP packets. A few seconds later, HGW reloads.Workaround: Wait until the Telnet session times out before bringing back up the Ethernet interface or attempting the second PPP session.
- CSCdp12094
When a gateway receives an alert from the ISDN network, it might not send an H225 alert message to the originating gateway to indicate a ring signal.
Workaround: Do not configure ISDN alert-end-to-end.

- CSCdp13466
ISDN Layer 2 might not come up if you have enabled Link Access Procedure, Balanced (LAPB) encapsulation.
Workaround: Enter the **no fair-queue** interface configuration command on the BRI interface.
- CSCdp16265
When using virtual private dial-up network (VPDN) callback, the tunnel might close without Layer 2 Tunnel Protocol (L2TP) dialout. There is no workaround.
- CSCdp17537
A Cisco router might reload with a bus error related to X.25 switching at PC 0x60A3DCB8, address 0xD0D0D41. There is no workaround.
- CSCdp18468
If you are switching an X.25 call through ISDN, and the call is cleared, no more ISDN calls will be issued for other X.25 call requests from the dialer interface. There is no workaround.
- CSCdp20697
If you have enabled both **atm multipoint-signalling** (interface configuration command) and **ip ospf network {point-to-multipoint}** (interface configuration command) on an ATM interface with the ATM multipoint switched virtual circuit (SVC) root, the ATM multipoint SVC (MSVC) might not be reestablished correctly, and the IP OSPF neighbors do not come up. There is no workaround.
- CSCdp22525
A Called Line Address Modification Notification (CLAMN) facility might not be present in an X.25 call confirmation packet that is within a hunt group. There is no workaround.
- CSCdp24563
Permanent Virtual Circuit (PVC) bumping does not function properly if you configure a VC that is down to be protected and then make it not protected again.
Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the subinterface.
- CSCdp26249
When IP packets (for example, OSPF) or 1483 packets trigger the creation of an ATM multipoint switched virtual circuit (SVC), the higher layer will see a lack of connectivity. Entering the **debug atm sig-all** privileged EXEC command will show that either the switch rejects the SETUP message or that the local timers expire, and the connection is released locally.
Workaround: Disable multipoint signalling on the interface by entering the **no atm multipoint-signalling** interface configuration command.
- CSCdp27204
When voice and data (such as FR EEK) are configured on a Frame Relay permanent virtual circuit (FR PVC), Frame Relay fragmentation and traffic shaping need to be configured at the same time. The following is an example configuration:

```
interface serial0
  encapsulation frame-relay
  frame-relay traffic-shaping
  frame-relay interface-dlci 16
class eek
```

vofr

```
map-class frame eek
  frame-relay end-to-end keepalive mode bidirectional
  frame-relay fragmentation
```

There is no workaround.

- CSCdp27902

A Cisco AS5300 access server using Group-Async Interfaces and Virtual Templates might terminate dialup links when Link Quality Monitoring (LQM) Link Quality Reports (LQRs) are received. This situation occurs when the local router is configured for LQM, but the remote side is not. There is no workaround.

- CSCdp27936

The configuration for X.25 hunt groups might be saved out of order, which prevents the installation of the X.25 routes that depend on those hunt groups.

Workaround: Manually add the X.25 routes back to the running configuration by entering the **copy startup-config running-config** command.

- CSCdp28607

A Cisco router that is running Cisco IOS Release 12.0(6.5)T and later releases might experience traceback errors on interfaces where Multilink PPP encapsulation was removed before weighted fair queueing (WFQ) was added.

Workaround: Shut down the interface before issuing the **no ppp multilink** interface configuration command or the **fair-queue** interface configuration command.

- CSCdp29684

If there are calls that are up, and the signalling controller (SC) does a switchover, some existing active calls are dropped on the network access server. There is no workaround.

- CSCdp30421

A Cisco router might reload if more than one active link is present as part of a bundle in a multilink group interface, and these links are unconfigured from the multilink group interface when the **no multilink-group group-number** interface configuration command and then the **'no interface multilink group-number** global configuration command are entered to remove the multilink interface.

Workaround: Perform a shutdown on all interfaces, and remove each group member. Then, shut down and remove the multilink interface.

- CSCdp42263

A Cisco 7206 router that is running Cisco IOS Release 12.0(8.0.1)T might experience a software forced reload. There is no workaround.

- CSCdp42274

A Cisco 7200 series router might exhibit the following error messages:

```
%IPFAST-2-PAKSTICK: Corrupted pak header for ATM2/0, flags 0x80 Traceback=
60361750 60314134 6031AE38
```

```
%IPFAST-2-PAKSTICK: Corrupted pak header for Virtual-Access6, flags 0x80
-Traceback= 603617EC 6065A270 60314134 6031AE38
```

There is no workaround.

- CSCdp42593
A Cisco AS5300 access server with the Q Signalling (QSIG) overlapping feature installed might start proceeding with dial-peers immediately after the first digits are matched. For example, number 12345 matches the dial-peer 1T. There is no workaround.
- CSCdp44888
A Cisco AS5300 access server with **no service align detect** configured will reload if you enter the **no pri-group** command on a controller that has no pri-group configuration.
Workaround: Enable **service align detect** in configuration mode. This will prevent the reload, but might result in an error message for accessing invalid memory.
- CSCdp44921
If you are running SNA switching with a Fast Ethernet connection to the host, the connection will function normally until an UNBIND is sent at the end of the user session. The UNBIND rsp is sent to the non-canonical (Token Ring format) MAC address; it is not recognized by the CIP, and the Logical Link Control (LLC) session pauses indefinitely.
Workaround: Use a MAC address that bit-swaps back to itself (such as 0000.6666.6666).
- CSCdp44953
After you reload a Cisco router, the PPP virtual template command protocol disappears under the VC Class ATM. This condition causes the PPP sessions to lose their binding with the virtual template. There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(7)T

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(7)T. This section describes severity 1 and 2 caveats and select severity 3 caveats.

Access Server

- CSCdm55659
The CT1 PRI on the double-density version of a Cisco AS5300 series access server might not operate properly when it is configured with a channel group and Frame Relay encapsulation on the serial port. The following error message might result when you configure the channel group:

```
23:31:18: ASSERTION FAILED: file "../as/if_as_pm7366.c", line 1291 23:31:18:
ASSERTION FAILED: file "../as/if_as_pm7366.c", line 1491
```


There is no workaround.
- CSCdm93937
When an AS5300 series access server is configured to transfer modem history events to a Syslog server, the router might reload if it received multiple V.110 calls.
Workaround: Configure the access server to not send messages to a Syslog server.

Basic System Services

- CSCdm43730
A Cisco router might reload with a bus error at PC 0x60215D90, address 0xC0F14D34. There is no workaround.

- CSCdm45305
On a Cisco MC3810 router, comfort-noise generation cannot be disabled.
Workaround: Disable voice activity detection (VAD) because comfort-noise is only applicable when VAD is engaged.
- CSCdm50233
The command-line interface (CLI) **voice class permanent** command has been restored. However, the CLI **voice class codec** command is still not working. There is no workaround.
- CSCdm51918
After configuring a named EXEC accounting method list, a Cisco router might lose part of the configuration, and the router will display an UNKNOWN-MODE configuration prompt when you try to configure interfaces.
Workaround: Remove any named EXEC accounting method lists, and reload the router.
- CSCdm52317
The **fax-rate {disable}** command in the dial-peer configuration does not work. Fax-relay is used to carry faxes instead of simple pass-through in the case of G.711 or G.726 adaptive differential pulse code modulation (ADPCM). Use of fax-relay restricts a Cisco 3810 router to a maximum of 12 calls instead of 24 calls when using G.726. There is no workaround.
- CSCdm54680
The nas-speed attributes might appear twice in the accounting STOP records. There is no workaround.
- CSCdm74850
A Cisco 3640 router that is running Cisco IOS Release 12.0(3c) cannot load large configurations (over 4000 characters and approximately 70 lines) in Async-group. There is no workaround.
- CSCdm80864
Entering the **backup interface bri 0** command breaks the **tdm-group** command under the T1/E1 controllers in Cisco IOS Release 12.0(5)XK. Removing the command, saving the configuration to NVRAM, and reloading does not solve the problem. You must either enter the **write erase** command and reload, or set config-reg to 0x42 to ignore NVRAM on bootup and then add the configuration minus the **backup interface bri 0** command.
Workaround: Disable ISDN backup.
- CSCdm84095
Accounting record is sent to both the network access server and the home gateway for the same dialing-in user when the network access server and the home gateway are connected via a Layer 2 Forwarding (L2F) tunnel. Accounting is sent to two different RADIUS servers. There is no workaround.
- CSCdp23786
A Cisco router that is running Cisco IOS Release 12.0(7)T cannot execute boot configuration commands from Flash, and exhibits the following error message:

```
%Error opening nvram:/startup-config (File system is in an inconsistent state)
```


When this message is displayed, no configuration is loaded. If you enter the **copy startup-config running-config** command and then enter the **no shutdown** command, the router will come back on line. There is no workaround.

EXEC and Configuration Parser

- CSCdm57527

Memory gets fragmented over a period of time when the output modifiers “|” are used. The memory allocated to the convergence sublayers used in pipeline stuffs must be deallocated properly. There is no workaround.

IBM Connectivity

- CSCdp00456

A Cisco router might reload when creating a circuit history for a data-link switching plus (DLSw) circuit.

Workaround: Disable circuit history logging by entering the **no dlsw history-log** command.

- CSCdp09919

Remote source-route bridging (RSRB) might change frame types. This situation occurs on Cisco routers that are running RSRB where one side of the RSRB is running Cisco IOS Release 11.0, and the other side is running Cisco IOS Release 12.0. The frame that is moving along the source-route translational bridging (SR/TLB) and RSRB bridge will be changed from an Ethernet Type II frame to an IEEE802.3 Ethernet frame.

Workaround: Configure the 90-compatible option by entering the **source-bridge transparent ring-group pseudo-ring bridge-number tb-group [90-compatible]** global configuration command.

Interfaces and Bridging

- CSCdm06860

Cisco IOS Release 11.1(24)CC might return a wrong value for Management Information Base (MIB) object cardType for PA-POSSW-MM/SM port adapters due to the Simple Network Management Protocol (SNMP) agent in the Cisco IOS Release 11.1(24)CC. Values for PA-POSSW 401 are returned instead of values for PA-POSSW 564 and PA-POSSW 564. There is no workaround.

- CSCdm19573

A Cisco 7200 series router that is running Cisco IOS Release 11.1(22)CC or Cisco IOS Release 11.1(25)CC with a PA-CT3 might experience problems with local-area transport (LAT) services under the following conditions:

If you are using transparent bridging with LAT enabled on a serial interface, you might not see LAT services when entering the **show lat service** command, even when the remote link (also using transparent bridging with LAT enabled) is advertising LAT services. There is no workaround.

- CSCdm42070

A Cisco 7200 series router that is running Cisco IOS Release 12.0(4)T reloads immediately if the controller e1 (4/0) is shut down.

The same three tracebacks are displayed:

```
Stack trace from system failure: FP: 0x618EB758, RA: 0x601D5A0C FP: 0x618EB788,
RA: 0x603DB0DC FP: 0x618EB7D0, RA: 0x603E6654 FP: 0x618EB828, RA: 0x6042D8C4 FP:
0x618EB840, RA: 0x6042D8B0
===== Show Alignment ===== Alignment data for: 7200
Software (C7200-IS-M), Version 12.0(4)T, RELEASE SOFTWARE (fc1) Compiled Thu
29-Apr-99 06:16 by kpma
No alignment data has been recorded.
Total Spurious Accesses 2, Recorded 2
Address Count Traceback 0 1 0x601D5A00 0x603DB0DC 0x603E6654 0x6042D8C4
0x6042D8B0 F60 1 0x601D5A04 0x603DB0DC 0x603E6654 0x6042D8C4 0x6042D8B0
=====Process Level Stack Trace=====
-Traceback= 601D5A0C 603DB0DC 603E6654 6042D8C4 6042D8B0
```

There is no workaround.

- CSCdm61866

A Cisco router that is running Cisco IOS Release 12.0(04a) might receive the following alignment error messages on dot1q over Internetwork Packet Exchange service access point (IPX SAP):

```
%ALIGN-3-CORRECT: Alignment correction made at 0x605B8E70 reading 0x63E5A6F1
%ALIGN-3-TRACE: -Traceback= 605B8E70 60095714 60095700 00000000 00000000 00000000
00000000 00000000
```

IPX SAP is affected only when dot1q encapsulation is involved (such as when IPX SAP is configured on a dot1q interface).

These alignment error messages do not affect connectivity or cause packet loss. There is no workaround.

- CSCdm88103

On a Cisco router that is running Cisco IOS Release 12.0(05)T when integrated routing and bridging (IRB) is enabled and AppleTalk routing only is enabled at the interface level, AppleTalk routing might not work properly. AppleTalk broadcasts will not be seen on an interface, so the router will not see neighboring AppleTalk routers, will not receive routing updates, and will not be able to process AppleTalk Address Resolution Protocol (ARP) packets. Some AppleTalk packets might actually be bridged to other AppleTalk routed interfaces in which the bridge group corresponding with the Bridge-Group Virtual Interface (BVI) is defined.

Workaround: Define an additional AppleTalk cable range (or address) and AppleTalk zone on the BVI.

- CSCdp12228

When a cable is disconnected from a Gigabit Ethernet Interface Processor (GEIP) interface port, a Cisco router that is running Cisco IOS Release 12.0 S or Cisco IOS Release 12.0 T might not report the link down event, and the interface stays up. There is no workaround.

- CSCdp18313

A Cisco 7206VXR router that is running Cisco IOS Release 12.0(6.5)T2 and has a network processing engine (NPE)-300 network processing engine might reload with a bus error. There is no workaround.

IP Routing Protocols

- CSCdm34431

An RSP4 Route Switch Processor (RSP) that is running Cisco IOS Release 12.0(3.6)T or Cisco IOS Release 12.0(4)T might reload with the following error message if you enter the **copy tftp running** command to update the configuration while the Versatile Interface Processor (VIP) or RSP is under a heavy traffic load:

```
ipfib_policy_forward vip_ip_fib_flow amdfe_rx_interrupt s_amdfe_check
```

This situation occurs when the RSP is running with a VIP2-50, a Fast Ethernet port adapter, and a PA-A3 port adapter and is configured with distributed Cisco Express Forwarding (dCEF), policy routing, and NetFlow.

Workaround: Avoid reloading the configuration with the **copy tft running** command.

- CSCdm52114

A bus error at PC ipmcast_nat address 0x86022BD3 might occur when IP multicast is set up on a tunnel with Network Address Translation (NAT). There is no workaround.

- CSCdm84348

After reloading BGP-3-BADROUTEMAP, bad parameters in the **bgp dampening [route-map name]** command might be logged every minute on Cisco IOS Release 12.0(5)T. This situation does not occur with Cisco IOS Release 12.0(4)T). Entering the **sho ip bgp dampened-paths** command shows the percent of dampening reconfiguration in progress.

Workaround: Enter the **no bgp dampening [route-map name]** command and then enter the **bgp dampening [route-map name]** command.

- CSCdp04586

A Cisco router that is running Border Gateway Protocol (BGP) might reload under a low memory condition with a bus error at PC bgp_attr2neighboras. Just before the reload, the router displays a message similar to the following:

```
%SYS-2-MALLOCFAIL: Memory allocation of 32728 bytes failed from 0x602A3FE4, pool Processor, alignment 0 -Process= "BGP Router", ipl= 0, pid= 107
```

There is no workaround.

- CSCdp05931

Border Gateway Protocol (BGP) might not send the default route to its neighbor when the router is configured with the **default-information originate** command. There is no workaround.

- CSCdp08311

A Cisco Router that is running Cisco IOS Release 12.0(6.4)T will not interoperate correctly in Designated Subnet Bandwidth Manager (DSBM) elections with a router that is running other Cisco IOS releases and might not interoperate with non-Cisco IOS DSBM or Subnet Bandwidth Manager (SBM) implementations.

In Cisco IOS Release 12.0(6.4)T, the L_AM_DSBM message is incorrectly formatted and validated. A valid incoming message is ignored by Cisco IOS Release 12.0(6.4)T, and an invalid message is ignored by other releases. The effect is that two routers on the same LAN operate as though they have won the DSBM election: one of the Cisco IOS Release 12.0(6.4)T routers, and one of the others. There is no workaround.

- CSCdp09342

In some circumstances, Enhanced Interior Gateway Routing Protocol (EIGRP) will not automatically install and advertise PPP host routes created through dial-in.

Workaround: Enter the **redistribute {connected}** command under EIGRP on the router receiving the dial connections.

- CSCdp18787

A Cisco router that has tag switching enabled and is running Cisco IOS Release 12.0(5)T might reload if a tag advertisement appears in a certain time window when a related routing update takes place. An ATM interface transition might cause this condition. There is no workaround.

- CSCdp31355

When importing between two VPN routing/forwarding instances (VRFs) on the same service provider edge router (PE), the imported paths will have the wrong table ID and be set to the table ID of the original VRF. There is no workaround.

- CSCdp41674

A Route Switch Module (RSM) that is running Cisco IOS Release 12.0 T and is configured for IP routing on a Token Ring VLAN with the IP directed broadcast option enabled might send out subnet broadcasts that it receives on its own subnet back to this same subnet.

Example: The RSM receives the subnet broadcast 10.10.10.255, and the RSM IP address is 10.10.10.1/24. The RSM will send back out on its own subnet a broadcast to the destination IP address 255.255.255.255, which is incorrect. On Layer 2, this frame goes to the destination MAC address ffff.ffff.ffff and is sent as an explorer on the Token Ring. The RSM should not do anything with the IP subnet broadcast as long as it is received on the interface that is directly connected to the router.

Workaround: Create an access list and disallow subnet broadcasts of the router subnet to enter the RSM.

Example:

```
interface vlan xxx type trbrf
ip address 10.10.10.1 255.255.255.0
.
.
ip access-group 101 in

access-list 101 deny ip any host 10.10.10.255
access-list 101 permit ip any any
```

ISO CLNS

- CSCdm61381

A Cisco 2500 series router that is running Cisco IOS Release 12.0(06)TPI or Cisco IOS Release 12.0S might reload if you enter the **no router isis [tag]** command. There is no workaround.

Miscellaneous

- CSCdk70788

An AS5800 T1 controller does not go off hook after receiving ani-dnis digits when configured for channel-associated signalling (CAS) with the **cas-group channel timeslots range type e&m-fgb mf ani-dnis** command. No calls can be placed via a T1 line with this configuration. There is no workaround.

- CSCdm03885

A Cisco AS5800 series router shelf might have difficulty distinguishing which digital signal level 0s (DS-0) are busied-out and which DS-0s are pending busy-out after you enter the **busyout shelf/slot** command on a CT3 controller. The result is that the CT3 might never get all of the DS-0s busied out.

Enhanced Cisco AS5800 series router DS-0 busy-out functionality for both Primary Rate Interface (PRI) and channel associated signalling (CAS) includes a modem reserve pool in the event that large number of users online have large volumes of call transitions. This functionality provides protection against failure due to modems being unavailable during the call transitions (recycling a modem after a call drop can take up to 10 seconds, during which time the modem is not available). The enhanced DS-0 busy-out functionality prevents calls from landing on the network access server during transition periods. There is no workaround.

- CSCdm09656

After you load an image on a Cisco 7500 series router that is running Cisco IOS Release 12.0 S or Cisco IOS Release 12.0 T, entering the **no shutdown** command on a T1 controller that is up might cause the T1 controller to go down. Channels created under that controller also go down. This situation only happens on a T1 controller and does not occur on a Cisco 7200 series router.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the T1 controller. If this workaround fails, perform a microcode reload to bring the controller back up.

- CSCdm18910

When port information is passed from an Layer 2 Tunnel Protocol Access Concentrator (LAC) and the **vpdn aaa attribute nas-port vpdn-nas** command is configured, it should be mapped to correct the network access server Port-Type value. There is no workaround.

- CSCdm27062

Incoming modem calls to a Cisco 3640 router over BRI might intermittently fail to train up. A handset call will hear silence. There is no workaround.

- CSCdm36607

A Cisco Layer 2 Tunnel Protocol (L2TP) might drop a tunnel if certain control messages are lost between a Cisco L2TP Access Concentrator (LAC) and a Cisco L2TP Network Server (LNS). This situation will most likely occur on a congested network or one where frequent packet loss occurs. There is no workaround.

- CSCdm39879

If voice activity detection (VAD) is enabled on Voice Over Frame Relay (VoFR) or Voice Over ATM (VoATM) calls on a Cisco 3810 router, significant voice quality degradation might occur.

Workaround: Disable VAD by entering the **no vad** command in all VoFR or VoATM dial peers.

- CSCdm40165
When tearing a Cisco Layer 2 Tunnel Protocol (L2TP) session, the virtual private dialup network (VPDN) multihop router might reload when receiving a Call Disconnect Notification (CDN) message.
Workaround: Turn off VPDN multihop.
- CSCdm42426
If using virtual private dialup network (VPDN) home gateway (HGW) load sharing on a network access server, any HGW failing to response might cause the network access server to reset itself.
Workaround: Do not use HGW load sharing; use only a single HGW.
- CSCdm47307
IP Routing Information Protocol (RIP) configured on a Cisco 1720 router that is running Cisco IOS Release 12.0(4.6)T might not broadcast routing updates. There is no workaround.
- CSCdm48968
A communication problem can exist between a current gatekeeper image interoperating with a gatekeeper image running with expanded fields in the Location Request (LRQ) 12.0(05.00.02)T, 12.0(05.00.01)PI06, 12.0(4)XL. Each gatekeeper might not understand the LRQs of the other and will drop the LRQ request. The result is that some calls will fail if the LRQ needs to be forwarded and is dropped, causing address resolution to fail for that call.
This situation exists when you see an error message indicating decoding of Time To Live (TTL) field error from H225 ASN1 decoder when between two gatekeepers. There is no workaround.
- CSCdm49454
Certain timing conditions might cause a buffer leak when the **cable ip-broadcast-echo** command is enabled. There is no workaround.
- CSCdm52552
A Cisco AS5300 series access server that is running Cisco IOS Release 11.3(09)AA might experience problems with the E1 R2 pulse line signalling in a Fuji to Ericsson switch. There is no workaround.
- CSCdm55626
All packets might get dropped when traffic shaping is configured on the interface because the number of queues are reported incorrectly.
Workaround: Disable traffic shaping.
- CSCdm56058
Mobile IP will dynamically create and destroy tunnels during registrations. When there are no more users on a tunnel, the tunnel will be released and recycled for the next use. Each time the tunnel interface is reused, a global counter is incremented. When the counter reaches around 970, the hardware address (HA) will not be able to create any more tunnels because it performs as though there are too many tunnels created on the router.
Workaround: Reload the router to reset the counter.
- CSCdm57104
A Cisco AS5300 series access server that is running Cisco IOS Release 12.0(06)PI or Cisco IOS Release 12.0 T might get stuck after 20 hours of running the gateway with a bowie image. The server will not send out an interactive voice response (IVR) prompt after users dial in to the gateway. Debug csm voice will exhibit the following output:

```
VDEV_ALLOCATE: failed to allocate a device
VDEV_ALLOCATE: failed to allocate a device
VDEV_ALLOCATE: failed to allocate a device
ERROR: CSM_RX_CAS_EVENT_FROM_NEAT:(0103): EVENT_CALL_DIAL_I N: no modem is
available.
to NEAT:(cid0103) EVENT_CALL_IDLE for slot0 ctrlr1 chan1 b
There is no workaround.
```

- CSCdm57727

The fax relay domain specific part (DSP) firmware is not recomputing the National Science Foundation frame check sequence (NSF FCS) correctly when the NSF frame size is 50 bytes or greater. There is no workaround.

- CSCdm59465

A Cisco 7200 series router with a PA-A3 port adapter that is configured with per-virtual circuit (VC) queueing and that is running Cisco IOS Release 12.0(04)T or later releases experiences packets stuck in the per-VC queue. When a packet arrives and there are no more PA-A3 tx credits, the packet will be put in the per-VC queue for that VC. But because no buffer descriptions are circulating for that VC, the packets get stuck in the per-VC queue. This situation only occurs when the output is overloaded and 100 or more permanent virtual circuits (PVCs) are concurrently loaded.

Workaround: Enter the **clear interface** command, or enter the **shutdown** command followed by the **no shutdown** command. These commands must be entered on the main ATM interface, which might cause unaffected PVCs to be temporarily disrupted.

- CSCdm59854

SS-EVAL H.323 Registration, Admission, and Status (RAS) messages might be discarded when a gateway or gatekeeper receives messages that include fields with an object identifier whose value is larger than 2 bytes. This situation occurs because the Cisco gateway or gatekeeper code tries to decode the object identifier value as a type of short when in fact it can contain values in the range of a long.

This situation might occur with the beta version of Cisco IOS Release 12.0(5)T and has been fixed in the Cisco IOS Release 12.0(5)T. There is no workaround.

- CSCdm61257

A Cisco AS5300 series access server might stop working if the Hot Standby Router Protocol (HSRP) extended Management Information Base (MIB) is walked when a Bridge Group Virtual Interface (BVI) is configured. There is no workaround.

- CSCdm61675

A Cisco router might experience internally generated packets not being routed using Cisco Applications and Services Architecture (CASA). There is no workaround.

- CSCdm64005

A PA-T3 port adapter might exhibit a timing problem resulting in dropped packets. There is no workaround.

- CSCdm65525

Packets entering the output-hold queue of the pathfinder might not be flushed out. There is no workaround.

- CSCdm67456

The voice port module (VPM) on a Cisco 3600 series router that is running Cisco IOS Release 11.3(10)T or Cisco IOS Release 12.0 T might lock up with the following error message:

```
%C542-1-NO_RING_DESCRIPTOR: No more ring descriptors available
```

This situation might cause the VPM to fail. There is no workaround.

- CSCdm67662

On Cisco 7500 series routers that are running Cisco IOS Release 12.0(T), entering the **show crypto engine connection active** command might display incorrect data in the interface and in the IP address fields. This situation will occur if a Versatile Interface Processor (VIP)-based crypto connection is established that has the same connection ID as an already existing non-VIP-based crypto connection. This situation is a display problem, and will not adversely affect traffic. There is no workaround.

- CSCdm68546

When a cable modem (CM) goes offline with key expiration and BPI enabled, there might be problems with the CM status display in the cable modem termination shelf (CMTS). There is no workaround.

- CSCdm69595

Compression aim might not work with multicast packets on a Cisco 2600 series router that is running Cisco IOS Release 12.0(05.00.02)T. The router might exhibit the following symptoms with hardware compression enabled on a CT1 interface or any serial interface involved in IP multicast routing:

- The compression module keeps going up and down consistently and frequently if **ip mroute-cache** is enabled.
- The serial i/f flaps with 1mg bps multicast packets.
- On the decompression router and the receiving router, the CPU utilization is 99 percent due to packets being process switched. The incoming frames drop rate is as high as 30 percent and all frames get process switched.

Workaround: Use software compression or no compression at all.

- CSCdm72383

The Synch Status column in the output of the **show switch connections** command displays a mismatch for all or a few connections even though the connections are good and traffic passes through them.

If the permanent virtual circuit (PVC) legs of connections are added using the **pvc** command, then the virtual circuit descriptor (VCD) is chosen automatically for those PVCs. If the Route Processor Module (RPM) is reloaded then these VCD values might change. If they do change, then those connections will appear in the mismatched state.

Workaround: Enter the **atm pvc** command and specify the VCD value explicitly in the command. Enter the **show switch connections nextvcd** command to determine a VCD value that can be used with the **atm pvc** command.

In the event that the **pvc** commands were used and some of the connections went into the mismatched state, fix the connections by adding the affected connections again. If all the connections are affected and all of them are in the mismatched state, add the connections by entering the **copy startup-config running-config** command.

- CSCdm73358
If modems send data with an odd MAC header length, Dynamic Host Configuration Protocol (DHCP) requests might be filtered out, so the modems cannot obtain an IP address. The modems will be stuck in init(rc) state. There is no workaround.
- CSCdm74152
A Cisco router that is running Cisco IOS Release 12.0(4.6)T through 12.0(5)T might experience problems with fast switching if Cisco express forwarding (CEF) is disabled.
Workaround: Enable CEF, and then disable CEF to remove it from the unwanted interfaces.
- CSCdm75198
The DD cache implementation results in memory loss, which will eventually result in the system reloading.
Workaround: Turn off DD caching by entering the **no ip dir cache** command.
- CSCdm75827
When using a dialer interface with ISDN and Routing Table Protocol (RTP) header compression, the compression configuration is not copied from the dialer interface to the physical interface on call startup, causing packets to not get compressed and compression statistics to not be incremented. There is no workaround.
- CSCdm76565
When the Dynamic Host Configuration Protocol (DHCP) client makes the DHCP request, the DHCP server returns the request. However, when the return packet is going through the router, the router is using 0.0.0.0 as the giaddr address when it should use the router Ethernet address that is connecting to the DHCP client. There is no workaround.
- CSCdm77892
With named access lists, the mapping class-map access control lists (ACL) might disappear. For example:
Before reload: class-map myclass match access-group toto
After reload: class-map myclass match none
Workaround: Use numbered ACLs.
- CSCdm80141
Cisco IOS Release 12.0(5)T incorrectly recognizes a digital signal level 3 (DS3) ATM Interface Processor (AIP) interface as an E3 AIP interface. There is no workaround.
- CSCdm81054
An IP Security (IPSec) router might configure a client with an IP address once each time IPSec Security Associations (SAs) are set up. It should do so only once per Internet Key Exchange (IKE) SA setup. Also, if the router initiates the first IPSec SA, it is not properly configuring the client before initiating the IPSec SA. There is no workaround.
- CSCdm82594
Some internal registers might not correctly update when the link goes down.
Workaround: Upgrade to Cisco IOS Release 12.0(7)T.

- CSCdm83396

If the endpoint for the Tunnel Endpoint Disc (TED) probe is the same as the protected router, the router will treat it as an initial Internet Key Exchange (IKE) message and not a probe, and the router will eventually fail.

Workaround: Configure the routers so that the access-list specifies the crypto endpoint to be some router or host beyond the protected router (and not the protected router).

- CSCdm85656

The size of the boothelper Cisco IOS Release 12.0(7)S c7200-boot-mz image has grown close to or past the storage capacity of the 4 MB boot flash memory. To remedy this situation, Cisco has reduced the size of the Cisco IOS Release 12.0(7)S c7200-boot-mz image to 2935880 bytes. The Port Adapter Spatial Reuse Protocol (PA-SRP) support has been removed from the Cisco IOS Release 12.0(7)S c7200-boot-mz image to achieve this size reduction. There will also be no new PA support added to the c7200-boot-mz image after Cisco IOS Release 12.0(7)S, in order to minimize the growth in size.

The following boot messages regarding the PA-SRP normally appear only if the Cisco IOS Release 12.0(7)S c7200-boot-mz image is booting up as the running image:

```
%PA-3-NOTSUPPORTEDBYLOADER: Port Adapter type 206 in bay X is not supported by this boot loader:
```

```
%PA-3-DEACTIVATED: port adapter in bay [X] powered off.
```

where X = the odd slot number occupied by the double-width PA-SRP.

There is no workaround.

- CSCdm86496

If you do not configure the port number while configuring the gatekeeper in the gateway, then the port is automatically set to 1718. After the Gateway Request (GRQ) is sent, the GCF is received from the gatekeeper. This message is taken as a spurious message (different source port 1719) and so the RRQ is not sent.

Workaround: Configure the port as 1719 while configuring the gatekeeper in the gateway.

- CSCdm87210

In Cisco IOS releases prior to Cisco IOS Release 12.0(7)T, IP Security (IPSec) images for the Cisco 805 router do not support the virtual private dial-up network (VPDN) feature. There is no workaround.

- CSCdm88415

If you assign the spectrum group to more than 16 upstreams per UBR7200, other upstreams might not get a frequency assigned and will result in a down state.

Workaround: Assign a fixed frequency to upstreams that are in a down state.

- CSCdm90364

For the Call Completion to Busy Subscribers (CCBS) feature, when PBX sends a PROGRESS message, the voice cut-through does not happen. So, although CCBS does work, the message played to inform the caller that he or she will get a ringback when the caller on-hook is not heard by the caller. There is no workaround.

- CSCdm91048

In Cisco IOS Release 12.0(5)T, when Context-Based Access Control (CBAC) is configured, http traffic is denied even though the **ip inspect http** command is not defined.

Workaround: Define the **ip inspect http name [inspect_list] java-list [#] access-list [#] permit any** command.
- CSCdm91091

During call setup using R2 Compelled, the call might fail to establish because the router fails to send the Group B signal to the PBX. There is no workaround.
- CSCdm91854

When you have source-route bridging (SRB) traffic between Token Ring LANE via a Route Switch Module (RSM), entering configuration mode on the RSM might result in the RSM not being able to forward the (SRB) frames.

This situation seems to only affect bridging with Token Ring LANE and not Token Ring Inter-Switch Link (TRISL) or local Token-Ring ports. There is no workaround.
- CSCdm93511

When using R2 signalling with the dual tone multifrequency Dialed Number Identification Service (DTMF DNIS) option enabled, the router will need to see DTMF digits within 30 seconds of the Seizure Acknowledgement. Otherwise, the router might present a fast-busy or secondary dialtone to the caller depending if DID or no DID is enabled on the matching peer. However, you should be able to configure your PBX to output digits within 4 seconds (preferably after 200 milliseconds).
- CSCdm94174

If a permanent virtual circuit (PVC) or virtual channel identifier (VCI) is added to a subinterface and then an identifier is added, the router might reload with memory corruption after exiting the configuration mode. There is no workaround.
- CSCdp00618

A Route Switch Processor (RSP) might reload while unprovisioning a channelized interface under heavy traffic. There is no workaround.
- CSCdp00957

The termination character for a Cisco AS5300 access server of the **dial-peer terminator * Now if character *** command is sent as the last character inside a dialed number (such as "011 420 2 714.....*"). The gateway does not accept it as a terminator and sends it as a part of the called party number.

The access server sends the * symbol through the IP network. When it arrives at the other PBX, the call is disconnected because the PBX does not understand the * symbol.

If you do not use the * symbol, the gateway always waits 5 seconds after the last digit or termination character. This timeout is configured by the **isdn overlap-receiving T302 5000** command. There is no workaround.

- CSCdp01651

If you try to download a static route from the RADIUS server when a user dials in, this static route displays the following syntax:

```
Framed-Route=158.76.96.80 255.255.255.248 0.0.0.0 1
```

On a Cisco AS5200 series access server that is running Cisco IOS Release 11.3, the route gets installed and the 0.0.0.0 part of the static route is replaced with the IP address that is assigned to the dial in client.

On a Cisco AS5300 series access server that is running Cisco IOS Release 12.0, the route gets installed in the routing table with a next hop address of 0.0.0.0. There is no workaround.

- CSCdp02233

A Cisco AS5300 series access server might reload while in Simple Network Management Protocol (SNMP) code due to strlen of cvIfCfgConnectionNumber. This cvIfCfgConnectionNumber string needs a \0 or string terminator at the end. This situation affects Voice over IP SNMP management. There is no workaround.

- CSCdp02448

If a Cisco AS5300 series access server is overloaded for several days (more than two calls per second per interface), it will run out of memory and require a reload. There is no workaround.

- CSCdp02586

SNA switch DLUR might fail LU-LU sessions at 0x08A00002 when uninterpreted PLU names are requested by the dependent LU. There is no workaround.

- CSCdp04510

Inter-Switch Link (ISL) that is configured on a Cisco router that is running Cisco IOS Release 12.0(4)T or Cisco IOS Release 12.0(05.05)T might not pass packets larger than 1446 bytes. There is no workaround.

- CSCdp06714

A virtual access interface that is reused via a recycling mechanism might cause memory leaks when configured with Cisco express forwarding (CEF) switching.

Workaround: Enter the **no ip cef** command to turn off CEF switching.

- CSCdp08114

A Cisco AS5800 series access server might reload when enabling resource pool management to work with SS7. The following error message is displayed:

```
AS5800 (config)#red
AS5800 (config)#res
AS5800 (config)#reso
AS5800 (config)#resource-pool
AS5800 (config)#resource-pool ? aaa Resource-manager AAA configuration call Call
treatment disable Disable resource manager enable Enable resource manager group
Group configuration profile Profile configuration
AS5800 (config)#resource-pool en
AS5800 (config)#
AS5800 (config)#resource-pool aaa prot local.
```

There is no workaround.

- CSCdp14267

On a Cisco AS5300 series access server, Voice over IP (VoIP) calls over T1/channel associated signalling (CAS) get timed out after the calls collect digits. There is no workaround.

- **CSCdp14502**

A Cisco router that is running Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) might forward Internet Control Message Protocol (ICMP) “unreachable” messages to the main routing table instead of sending them to the originating VPN routing/forwarding instance VRF. This situation prevents IP maximum transmission unit (MTU) discovery from working properly.

Workaround: Disable IP MTU discovery on the affected hosts.
- **CSCdp14765**

A Cisco router that is running fast switching (not Cisco express forwarding) and software crypto might display the following message:

```
%IPFAST-2-PAKSTICK: Corrupted pak header for FastEthernet0/ 1, flags 0x80
-Traceback= 6026398C 60EA7DE4 60E83840 60E82C04 6035E464 6035E450
%IPFAST-2-PAKSTICK: Corrupted pak header for FastEthernet0/ 1, flags 0x80.
```

There is no workaround.
- **CSCdp15649**

Interactive voice response (IVR) drops a call if you do not respond to the prompt for account number and the prompt times out. There is no workaround.
- **CSCdp15967**

All downstream packets might be process switched on virtual profile interfaces. There is no workaround.
- **CSCdp17553**

A Cisco router that is running Cisco IOS Release 12.0(6.5)T3 will reload when a crypto map is removed from the configuration.

Workaround: Save the configuration in a text file, edit the file, enter the **write erase** command on the router, and paste the edited configuration.
- **CSCdp17634**

If you enter the **show snas pu** command, the physical unit (PU) appears active on the Systems Network Architecture Switching Services (SNASw) but no link exists for the PU. When the PU connects to SNASw, it is rejected because SNASw already has an entry for that PU through that exchange identification (XID). There is no workaround.
- **CSCdp18279**

Entering the **no ip director server ip-address** or **no ip director server ip-address** commands, which remove the remote server from the list of servers receiving regular verification connections, might cause the system to reload. There is no workaround.
- **CSCdp19680**

When you configure output interfaces with fast switching on a Cisco 1700 series router, IP Security (IPSec) traffic might report replay errors for certain packets because IPSec decryption connection identifiers are not saved correctly when the packets are coalesced from protocol control information (PCI) memory to DRAM. The replay errors usually appear in incoming traffic. A Media Access Control (MAC) verify failure error might also appear. There is no workaround.

- CSCdp19753
In Cisco IOS Release 12.0 T Cisco express forwarding (CEF) will not work with bundle virtual circuits (VC)s if you use subinterfaces that are part of the same physical interface. There is no workaround.
- CSCdp20420
A SNA switch that is using High-Performance Routing (HPR) protocol, might have difficulty running in routers with relatively small amounts of input/output (I/O) memory (less than 2 MB). There is no workaround.
- CSCdp21424
A Cisco 7200 or 7500 series router with a POTENT port adapter might exhibit the following error message:

```
%LINK-2-INTVULN: In critical region with interrupt level=0, intfc=Serial3/0:0
```

There is no workaround.
- CSCdp29665
When calls are redirected multiple times in the telephone network before arriving at a Cisco AS5300 access server by a 5ESS PRI, the redirecting number that is tunneled by H.323 will be the Original Called Number (OCN) (the first party to forward the call) rather than the Redirecting Number (RDN) (the last party that forwarded the call directly to the Cisco AS5300). But services that access the RDN will need the final RDN rather than the OCN. There is no workaround.

Novell IPX, XNS, and Apollo Domain

- CSCdm56600
Images without the Internetwork Packet Exchange-Enhanced Interior Gateway Routing Protocol (IPX-EIGRP) subsystem will have high CPU load due to continuously attempting to process EIGRP-specific service information when no information is present. There is no workaround.

Wide-Area Networking

- CSCdk82129
On a Cisco AS5800 series access server, a PRI connection connected to a Synchronous Optical Network (SONET) network is not ignoring the microinterruption on the SONET ring when the SONET ring switches from one SONET ring to another for backup reasons. Due to this microinterruption, the ISDN Layer 2 will disconnect all users currently connected to the access server. There is no workaround.
- CSCdm12191
When running distributed Multilink PPP (MLP), the Versatile Interface Processor (VIP) might not return packet headers correctly, which will drain the VIP of all available memory.
Workaround: Perform MLP processing on the Route Switch Processor (RSP) by entering the **no ip route-cache distributed** interface configuration command. Note that entering this command will result in higher CPU utilization.

- CSCdm34468

In Cisco IOS Release 12.0(3.6)T and later releases, when a dialer interface is configured and the **dialer pool** command is used to specify dialer profiles (that is, there is no **dialer remote-name** command), and the configuration is stored in startup-config and the router rebooted, some dialer commands such as **dialer hold-queue**, **dialer idle-timeout**, and **dialer caller** might disappear from the configuration after rebooting, even though they are still present in the startup-config.

Workaround: Configure the **dialer remote-name** command on the failing dialer interface. In interface configuration mode, enter:

```
dialer remote-name foo
```

For purposes of this workaround, **foo** may be any name.

After applying the workaround for this problem, you need to use the command-line interface (CLI) on the router to add the missing commands, then save the running-config to startup-config. The order of the commands will be different after applying the workaround. If the commands are in the wrong order (as they will be if the configuration was saved before the fix was applied), the commands will disappear as if you did not apply the workaround.

- CSCdm36896

Cisco IOS Release 12.05T fixes the problem where Layer 2 Tunnel Protocol (L2TP)-specific configurations were not working properly when configured locally on a network access server and resource-pool was disabled.

- CSCdm37718

Because the router includes the Channel ID Information Element (DE) in the ALERTING and the CONNECT messages, the Siemens NI1 switch sends the STATUS message in accordance with section 6.3.5.2 of the Bellcore SR-NWT-001953 *ISDN Terminal Equipment on Basic Access Interfaces*. It is recommended but not required that the terminal equipment (such as the Cisco router) not include the Channel ID IE after the CALL_PROC. If the router does include this IE, the switch is supposed to ignore it and send a STATUS message.

Previously, if you received an unsolicited STATUS message from the switch, you would perform a call state comparison and if the call states were not the same you would release the call. When the call is still in the progressing call states, the progressing call states will not be equal. How to handle the STATUS message under certain cause conditions such as invalid IE or mandatory IE missing is an implementation option.

Workaround: If the switch sends a complaining STATUS message about including optional IEs, allow them to be included and to determine if they wish to terminate the call. This option is implemented only for call progressing states four through nine.

- CSCdm44636

Layer 2 Tunnel Protocol (L2TP) sends an SLI prematurely. This situation can cause incorrect Link Control Protocol (LCP) values such as Asynchronous Control Character Maps (ACCMs), which will break interoperability with some L2TP Access Concentrators (LACs) serving asynchronous lines. There is no workaround.

- CSCdm44736

Outbound Data Over Voice (DOV) calls fail with the following error message immediately after the call has successfully gone through at the Q.931 layer:

```
ISDN BR0: HOST_CONNECT: VOICE ERROR 0x3A: bchan 0, call id 0x8001
```

There is no workaround.

- CSCdm45278
Incoming ISDN BRI calls might cause a Cisco router to reload when Channel ID 0x88 is received in the incoming SETUP messages. There is no workaround.
- CSCdm47748
A Cisco router that is running Cisco IOS Release 11.1(25)CT with tag switching and Intermediate System-to-Intermediate System (IS-IS) configured might reload due to bus error. The PC at the reload time will look corrupted. The reload will occur after displaying the following error message:

```
%UTIL-3-TREE: Data structure error--attempt to remove an unthreaded node from a tree
```

There is no workaround.
- CSCdm47927
Command line interface (CLI) Callback might not work on a Cisco router that is running Cisco IOS Release 12.0.(4)T. ISDN caller and dialer caller with and without dialer profiles do not solve the problem. The call connects but the router neither disconnects the call nor dials back. There is no workaround.
- CSCdm48365
You might experience problems connecting to DMS100 and NI1. The **debug ISDN Q931** command displays the following error message:

```
invalid Channel ID
```

The DMS100 and NI1 switches reject the call because the Channel ID IE is formatted incorrectly.
Workaround: Update to a release containing the fix, which can be located by Throttle Tracker on CCO.
- CSCdm55097
When you enable **dcef** on an ATM interface with an ATM bundle configured, packets that need to be sent over the bundle get dropped due to no adjacency. There is no workaround.
- CSCdm52736
For Redundant Link Manager (RLM), where the nfas_d primary is unplugged on the E1, even if the signalling on RLM should not be involved, an NL_REL_IND message is sent to the ISDN module, which stops communicating with the Signal Channel (SC). There is no workaround.
- CSCdm78708
Asynchronous PPP callback is not correctly negotiated between two Cisco routers. The PPP negotiation fails during callback. There is no workaround.
- CSCdm84992
The Server Replication Protocol (SRP) feature might not be completely disabled when you enter the **no lane fssrp** command.
TLVs are still included in the LANE_JOIN_REQ which might cause compatibility issues with LAN Emulation Server (LES) implementations that do not support these TLVs.
Workaround: Upgrade Cisco LAN emulation Server/broadcast and unknown server (LES/BUSs) to Cisco IOS Release 11.2(13) for the routers and upgrade to Cisco IOS Release 3.2(7) or later for the Catalyst 5000 LANE models. The upgrades will cause the Cisco LESs to ignore the TLVs.

- CSCdm89069

When Multilink PPP (MLP) is used and the peer sends MLP encapsulated fragments or packets, MLP frequently discards the inbound frames. This situation is particularly obvious when the peer is fragmenting packets because the router will drop a fragment and consequently drop an entire inbound network layer packet due to inability to reassemble a complete packet from the fragments. This situation becomes particularly noticeable on slower speed links (such as typical asynchronous connections) where the overall packet loss rate can become quite high. This problem occurs because the MLP lost fragment timer expires prematurely, which causes MLP to declare inbound fragments as “lost” within a few milliseconds instead of waiting for at least 1 second for expected frames. There is no workaround.

- CSCdm91170

Callback that is configured on a dialer interface might not work.

Workaround: Enter the **isdn caller** command, which will provide the same functionality as callback.

- CSCdp08283

On a Cisco router that is running Cisco IOS Release 12.0(5)T, LAN Emulation clients may use an incorrect value for the service data unit (SDU) size in their setup message to the LAN Emulation Server (LES). This situation might prevent the client from coming up. This situation only happens if the maximum transmission unit (MTU) on the subinterface is set for nondefault (greater than 1500).

Workaround: Use a MTU of 1500 on the sub-interfaces.

- CSCdp12115

Caller ID screening and CLI callback might not work on a Cisco 800 series router. There is no workaround.

- CSCdp13023

If you are using Always On/Dynamic (AO/D) ISDN and trying to negotiate link control protocol (LCP), all requests to negotiate the Link Discriminator will be rejected. There is no workaround.

- CSCdp19479

A Cisco router might experience a bus error and reload if you enable the ATM bundle on the PA-A3-OC3MM ATM port adapter. There is no workaround.

- CSCdp36025

The default number type and number plan for the Q Signalling switch type has been changed to “unknown” because when interworking with non-ISDN, the originating number type and number plan is unknown. There is no workaround.

Resolved Caveats—Cisco IOS Release 12.0(6)T

Cisco IOS Release 12.0(6)T was not released. Please see “Resolved Caveats—Cisco IOS Release 12.0(7)T” section on page 23.

Resolved Caveats—Cisco IOS Release 12.0(5)T

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(5)T. This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCdm50233

The **voice class codec** command does not function properly. However, the **voice class permanent** has been restored. There is no workaround.

Interfaces and Bridging

- CSCdm42070

A Cisco 7200 series router running the “c7200-is-m” software image in Cisco IOS Release 12.0(4)T reloads immediately if the E1 controller (4/0) is shut down. There is no workaround.

Miscellaneous

- CSCdm09656

In Cisco IOS Release 12.0 S and Release 12.0 T, after you load the image on a Cisco 7500 series router, issuing the **no shutdown** command on a T1 controller that is up causes the T1 controller to go down. Channels created under that controller also go down. This only happens with T1 and does not occur on Cisco 7200 series routers.

Workaround: Issue the **shutdown** command followed by the **no shutdown** command on the T1 controller. If this fails, perform a microcode reload to bring the controller back up.

- CSCdm27062

Modem calls to a Cisco 3640 router intermittently fail to train up. A handset caller will hear silence.

Workaround: Issue the **clear interface bri x/y** command to temporarily resolve the issue.

- CSCdm30103

A Cisco 1700 series router Fast Ethernet interface receives input errors when small packets (less than 200 bytes) are received at a time when the interface is receiving 500 packets per second and running fast switching. There is no workaround.

- CSCdm36607

L2TP tunnels between a Cisco AS5300 series access server and a Cisco 7200 series router might drop several times every hour. There is no workaround.

- CSCdm39879

If voice activity detection (VAD) is enabled on Voice over Frame Relay (VoFR) or Voice over ATM (VoATM) calls on a Cisco MC3810 multiservice access concentrator, significant voice quality degradation might occur.

Workaround: Disable VAD by placing a **no vad** statement in all VoFR or VoATM dialpeers.
- CSCdm40165

When tearing down an L2TP session, a VPDN multihop router might reload after receiving a CDN message.

Workaround: Disable VPDN multihop.
- CSCdm42426

If you use VPDN home gateway (HGW) loadsharing on a NAS, any HGW that fails to respond will cause the NAS reset itself.

Workaround: Do not use HGW loadsharing. Use a single HGW.
- CSCdm44249

Reusing the same customer edge (CE) address on two CEs connected to the same provider edge (PE), in different VPN routing/forwarding instances (VRFs), does not work properly when the link between the PE and CE is Ethernet. There is no workaround.
- CSCdm46169

When running RIP on a VPN interface, the provider edge (PE) router does not send out RIP updates. There is no workaround.
- CSCdm47307

If IP RIP is configured on a Cisco 1720 router running Cisco IOS Release 12.0(4.6)T, routing updates might not be broadcasted. There is no workaround.
- CSCdm49454

Under certain timing conditions, enabling **cable ip-broadcast-echo** can cause a buffer leak.

Workaround: Do not enable **cable ip-broadcast-echo** and **cable ip-multicast-echo**.
- CSCdm55626

Traffic shaping might not work. All packets can get dropped when traffic shaping is configured on the interface.

Workaround: Disable traffic shaping.
- CSCdm56394

Under certain circumstances, when redistributing routes, a Cisco router can incorrectly identify the routing protocol which originated a route. There is no workaround.

Wide-Area Networking

- CSCdm36896

L2TP specific configurations have no effect when configured locally on a NAS. This applies to Cisco IOS Release 12.0(5)T only. There is no workaround.

- CSCdm45278
Incoming ISDN BRI calls might fail at “process_dialer_command()” when “Channel ID 0x88” is received in the incoming setup messages. There is no workaround.
- CSCdm47927
CLI Callback might not work on a Cisco 3640 router running Cisco IOS Release 12.0(4)T. Calls connect, but the router never hangs up or dials back. There is no workaround.
- CSCdm48075
By default, LANE FSSRP is off on all subinterfaces and all LANE components.
Workaround: Issue the **lane fssrp** interface configuration command. This command recycles all LANE components on an interface and its subinterfaces.
- CSCdm49871
A Cisco router reloads when you deconfigure a routing protocol (for example, when you issue the **no ipx routing** command). The problem exists in Cisco IOS Release 12.0(3)T and Release 12.0(3)S and later releases. At least one Frame Relay interface must be configured and at least one Frame Relay map (an association between a DLCI and a level 3 protocol address) must be established by Inverse ARP.
Workaround:
 - (a) Disable Inverse ARP for the routing protocol to be deconfigured (for example, for IPX routing, use the **no frame-relay inverse-arp ipx dlc** interface configuration command).
 - (b) Clear the Frame Relay Inverse ARP cache using the **clear frame-relay-inarp** executive command.
 - (c) Remove the routing protocol from the router (for example, for IPX routing, use the **no ipx routing** global configuration command).

Resolved Caveats—Cisco IOS Release 12.0(4)T

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(4)T. This section describes severity 1 and 2 caveats and select severity 3 caveats.

Access Server

- CSCdk93347
Running dial-on-demand routing on the asynchronous interface causes a Cisco AS5200 access server to reload. There is no workaround.

Basic System Services

- CSCdk80074
Initialization fails for a Basic Rate Interface (BRI) that is connected to a Siemens HICOM PABX, leaving the Layer 1 status in “ACTIVE_ErrorInd.” There is no workaround.

IP Routing Protocols

- CSCdm10783

The **configure memory** command might cause a Versatile Interface Processor (VIP) to reload when access lists are configured. There is no workaround.

Miscellaneous

- CSCdk55110

When tunneling IPX over an IP tunnel, and when using an extended inbound access list for IP on the tunnel interface, the IPX traffic gets blocked by the access list.

Workaround: Add a **permit gre** statement in the extended access list.

- CSCdk69415

An RSP-based router running Cisco IOS Release 11.2(15a)P might stop IP traffic that passes through two Fiber Distributed Data Interface (FDDI) port adapters and is encrypted and decrypted on the VIP2-40. When this problem occurs the VIP locks up. Users cannot go to the VIP console and the VIP does not receive or send out any packets.

Workaround: Reload the microcode.

- CSCdk85615

There is no way to configure MICA modem lines on a Cisco 3640 router for dial-out only. The **modem dtr-active** command fails and displays the following error message:

```
NO DIALTONE
```

There is no workaround.

- CSCdm10790

After a Versatile Interface Processor (VIP) or Route Switch Processor (RSP) reloads, all E1 controllers on PA-MC-8E1/120 modules flap until the framing is toggled from NO-CRC4 to CRC4 and back again. Flapping occurs with PA-MC-8E1/120 port adapters connected to CPE devices running framing NO-CRC4. It has been seen in the following releases: Cisco IOS Release 11.1(21)CC, Release 11.1(23)CC, Release 11.1(24)CC, Release 12.0(2)XE1, and Release 12.0(3)T.

Workaround: Toggle the framing parameter on and off to stabilize the controller.

- CSCdm15356

If two Cisco routers are connected with parallel logic connections, and all the parallel interfaces are running RIP networks within the same major network, the routers will reload with the following error message:

```
System was restarted by bus error at PC
0x604D66BC[rip_redistribute_net(0x604d65e4)+0xd8], address
0xB0D0B19[[_start(0x60008000)+0xab0c8b19] rip_redistribute_net
rip_service_redist rip_process_workq rip_router r4k_process_dispatch
r4k_process_dispatch
```

There is no workaround.

- CSCdm15557

Timing adjustment during the ranging process should be more flexible.

Workaround: Allow timing adjustment to be configured per upstream.

Resolved Caveats—Cisco IOS Release 12.0(3)T

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(3)T. This section describes severity 1 and 2 caveats and select severity 3 caveats.

Basic System Services

- CSCdk57339

The **[no] atm rmon collect *group-num*** command does not properly take effect when invoked. The ATM-RMON feature (available only on the LS-1010 platform) is fully functional, except when you assign ATM interfaces to ATM-RMON collection groups. In this situation, you must set the associated MIB objects with SNMP. See the portSelTable definitions in the ATM-RMON-MIB.my MIB document for more information. There is no workaround.

IP Routing Protocols

- CSCdk70273

If there are more than 31 Open Shortest Path First (OSPF) interfaces, flooding does not work, starting from the 32nd OSPF interface. There is no workaround.

Miscellaneous

- CSCdk45102

The Token Ring Inter-Switch Link (TR-ISL) feature is currently not supported on either the Cisco 3620 router or the Cisco 3640 router. There is no workaround.

- CSCdk56804

The IP portion of an incoming call might not terminate correctly if the caller closes the connection. This situation is the result of rare timing conditions. There is no workaround.

- CSCdk67063

Airline Product Set (ALPS) P1024C data-link layer protocol (UTS) serial encapsulation can not be configured. There is no workaround.

- CSCdk76257

Data packets are not padded to the minimum length of 60 bytes in the downstream direction. This might cause runt packets to be transmitted to the Ethernet behind a cable modem if the cable modem software does not pad to the minimum packet length. (This condition was optional in earlier releases, but was recently changed in the specification and is now considered a caveat.)

In Cisco IOS Release 12.0 T, if Cisco Express Forwarding (CEF) switching is enabled, packets shorter than the minimum permitted packet size are corrupted during transmission and the modem receives packets with HCS errors.

Workaround: Disable CEF switching.

- CSCdk78616

Airline Product Set (ALPS) agent-set control units (ASCUs) are unable to forward data to the host systems. There is no workaround.

- CSCdk82659

PA-MCE1 and PA-MCT1 port adapters might experience port flapping when the bandwidth of the data that is directed at the port adapter is greater than the physical bandwidth of the port adapter interface when it is transmitting.

Workaround: Turn off keepalives to help reduce the amount of port flapping.
- CSCdk83974

DistributedDirector needs to be updated to include the latest fixes from the original Cisco IOS Release 11.1 IA branch. Further updates include the ability to handle more than eight IP addresses per host name, the ability to select on “MX” records as well as “A” records, and policy redirection. There is no workaround.
- CSCdk84528

If you change the dial shelf ID, a Cisco router might continuously reload. This condition might occur when you load the startup configuration from the TFTP server, or when you issue the **shutdown** command followed by the **no shutdown** command under the controller. There is no workaround.
- CSCdk85957

The following information only applies if the (cable) Media Access Control (MAC) header received from cable modems has an odd length. (So far, this caveat has only been observed by one modem vendor when Baseline Privacy is active.)

 - If you are running Cisco IOS Release 11.3 NA and flow switching is enabled, packets that are received from a cable interface and transmitted to another interface are corrupted. Also, several alignment errors are reported. There is no workaround.
 - If you are running Cisco IOS Release 12.0 and flow switching is enabled, but CEF switching is disabled, several alignment errors are reported (switching itself works). If CEF switching is enabled, packets that are received from a cable interface and transmitted to another interface are corrupted. Also, several alignment errors are reported. There is no workaround.
- CSCdk87454

If the Baseline Privacy Interface (BPI) is active, or registration requests contain BPI fields, each registration request causes a memory leak of approximately 50–100 bytes.

Workaround: Do not enable BPI, and configure **cable qos permission modems**.

Wide-Area Networking

- CSCdk41155

A Cisco router might fail to reply to an incoming Address Resolution Protocol (ARP) on the Bridged-Group Virtual Interface (BVI) when the ARP table is clean. The following error message appears if the **debug arp** command is enabled:

```
00:50:23: IP ARP req filtered src 10.1.1.254 0000.0c32.ed77, dst 10.1.1.1
0000.0000.0000 wrong cable, interface Virtual-Access
```

Workaround: To install the ARP entries, initiate traffic from the router and force an incoming ARP BVI reply.

- CSCdk71837

Due to the merge of new feature integration branches into Cisco IOS Release 12.0 T, outgoing voice BRI calls were broken except for the Cisco 800 series router platform. The cause was largely due to the addition of data over voice (DOV) support for Cisco 800 series routers. For the time being, this DOV feature has been made exclusive to Cisco 800 series routers so that normal outgoing voice calls are not affected. There is no workaround.

- CSCdk81819

After several incoming calls to a Cisco 803 router or a Cisco 804 router, the router cannot make any outgoing calls (manual or from the DDR), nor can the router hang up the calls. There is no workaround.

- CSCdk82536

When a Cisco 700 series router places a call to a Cisco 800 series router, the phone on the Cisco 800 series router continues to ring after the Cisco 700 series router hangs up on an unanswered call. There is no workaround.

- CSCdk85516

Outgoing ISDN calls might fail because the called party number information element (CPNIE) has a number type of “Unknown” and number plan identification (NPI) of “Unknown.” There is no workaround.

- CSCdk86423

The **mtu** interface command cannot accept a value less than 1500 bytes.

Workaround: For IP, use the **ip mtu** command.

Resolved Caveats—Cisco IOS Release 12.0(2)T

All the caveats listed in this section are resolved in Cisco IOS Release 12.0(2)T. This section describes severity 1 and 2 caveats and select severity 3 caveats.

IP Routing Protocols

- CSCdk37843

On some platforms, for example the Cisco 7200 series routers, Routing Information Protocol (RIP) does not get enabled on Token Ring interfaces. The output of the **show ip proto** command indicates “Reset all is OK.”

Workaround: Configure **router rip** on the router before configuring the address on the interface. A **shutdown** command followed by a **no shutdown** command might also bring up RIP on the interface.

- CSCdk52224

When you use sparse-mode Protocol Independent Multicast (PIM), the multicast tree might take a few minutes to stabilize after the routers are booted. During this period, “PATH” messages sent to multicast addresses are not delivered, and Resource Reservation Protocol (RSVP) path and reservation sessions are not established. This is a transient phenomenon that occurs only when the routers are being booted. After the multicast tree stabilizes, paths and reservations are established quickly. This problem does not occur in unicast or dense-mode multicast networks.

Workaround: Use sparse-dense or dense-mode PIM multicast, if possible.

Miscellaneous

- CSCdk38476

RADIUS accounting does not work if you have separate authentication and accounting servers. There is no workaround.

- CSCdk41902

An IP client might not be able to ping the Route Switch Module (RSM). This situation might occur during Token Ring virtual LAN (TR VLAN) configuration on the RSM. It is most common when the IP client sends an Address Resolution Protocol (ARP) without a routing information field (RIF), and then sends an ARP with a RIF. The situation might also occur if the Concentrator Relay Function (CRF) to which the client is connected is configured for source-route bridging (SRB).

Workaround: Change the CRF mode from SRB to source-route transparent bridging (SRT).

- CSCdk59879

A Cisco 1600 series 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.

Workaround: Turn off fast switching with the **no ip route-cache** command on the ISDN interfaces.

- CSCdk67834

Cisco 800 series routers configured for multilink and STAC compression experience a page leak after prolonged usage. This condition is rare (roughly 1 in 50 units experience it) and might take several days to manifest, depending on the number of calls. In this situation, performance degrades until the unit thrashes (that is, the router runs so slowly that no useful work is accomplished). This is accompanied by continuous and heavy blinking of the OK LED.

Workaround: Disable multilink or disable STAC compression. A soft or hard reset (for example, issue the **reload** command or power cycle) is the only way to clear the problem after it occurs.

Novell IPX, XNS, and Apollo Domain

- CSCdk52372

The Internetwork Packet Exchange (IPX) input process might run out of stack, causing a system reload or reduced performance. There is no 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.

This document is to be used in conjunction with the product specific release notes for Cisco IOS Release 12.0 T.

Access Registrar, AccessPath, Are You Ready, ATM Director, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Networking Academy, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, iQuick Study, iQ Readiness Scorecard, The iQ Logo, Kernel Proxy, MGX, Natural Network Viewer, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, RateMUX, ReyMaster, ReyView, ScriptShare, Secure Script, Shop with Me, SlideCast, SMARTnet, SVX, TrafficDirector, TransPath, VlanDirector, Voice LAN, Wavelength Router, Workgroup Director, and Workgroup Stack are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Collision Free, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document/website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (0008R)

Copyright © 1998-2000, Cisco Systems, Inc.
All rights reserved. Printed in USA.

