



Caveats for Cisco IOS Release 11.2 P

June 16, 2004

Text Part Number 78-6394-11 Rev. F0



Note

You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hard copy documents were printed.

This document lists severity 1 and 2 caveats for Cisco IOS Release 11.2 P, up to and including Release 11.2(26)P7. 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.



Note

Cisco IOS Release 11.2(26)P is the last scheduled maintenance release for Cisco IOS Release 11.2 P. TAC support will continue to be available. This caveats document will be the last caveats document published for Cisco IOS Release 11.2 P.

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 42.

How to Use This Document

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

- “Open Caveats” lists open caveats that apply to the current release and might apply to previous releases.
- “Resolved Caveats” lists caveats resolved in a particular release, but open in previous 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.



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

Copyright © 1998–2004. Cisco Systems, Inc. All rights reserved.

If You Need More Information

The most up-to-date documentation can be found on the web through Cisco.com and on the latest Documentation CD-ROM. These electronic documents might contain updates and modifications made after the paper documents were printed. For information on Cisco.com, see the “Cisco.com” section on page 43. For more information on the CD-ROM, see the “Documentation CD-ROM” section on page 42

For more information on caveats and features in Cisco IOS Release 11.2 P, see the following sources:

- *Dictionary of Internetworking Terms and Acronyms*—The *Dictionary of Internetworking Terms and Acronyms* document contains definitions of acronyms that are not defined in this caveats document.
- Bug Navigator II—If you have an account on Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. Access Bug Navigator II at <http://www.cisco.com/support/bugtools>, or from Cisco.com by logging on and selecting **Software Center: Cisco IOS Software: Cisco IOS Bug Toolkit: Bug Navigator II**.
- *Release Notes for Cisco IOS Release 11.2*—These release notes describe new features and significant software components for Cisco IOS Release 11.2. All features in Cisco IOS Release 11.2 are also in Cisco IOS Release 11.2 P.



Note Release notes are modified only 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 release notes that were most recent when this caveats document was published.

Release Notes	Cisco IOS Release	Revision Date
Release Notes for the Cisco 1000 Series Routers for Cisco IOS Release 11.2 P	Release 11.2(26)P	April 16, 2001
Release Notes for the Cisco 1600 Series Routers for Cisco IOS Release 11.2 P	Release 11.2(26)P	April 16, 2001
Release Notes for the Cisco 2500 Series Routers for Cisco IOS Release 11.2 P	Release 11.2(26)P	April 16, 2001
Release Notes for the Cisco 3600 Series for Cisco IOS Release 11.2 P	Release 11.2(26)P	April 16, 2001
Release Notes for the Cisco 4000 Series for Cisco IOS Release 11.2 P	Release 11.2(26)P	April 16, 2001
Release Notes for the Catalyst 5000 Series RSM/VIP2 for Cisco IOS 11.2 P Software Releases	Release 11.2(26)P	April 16, 2001
Release Notes for the Cisco AS5100 and AS5200 Access Servers for Cisco IOS Release 11.2 P	Release 11.2(26)P	April 16, 2001
Release Notes for the Cisco AS5300 Access Server for Cisco IOS Release 11.2 P	Release 11.2(26)P	April 16, 2001
Release Notes for the Cisco 7000 Family for Cisco IOS Release 11.2 P	Release 11.2(26)P	April 16, 2001

Resolved Caveats—Cisco IOS Release 11.2(26)P7

Cisco IOS Release 11.2(26)P7 is a rebuild of Cisco IOS Release 11.2(26)P. All caveats listed in this section are resolved in Cisco IOS Release 11.2(26)P7 but may be open in previous Cisco IOS releases.

- CSCdu53656

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

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

- CSCea28131

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

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

Resolved Caveats—Cisco IOS Release 11.2(26)P6

Cisco IOS Release 11.2(26)P6 is a rebuild of Cisco IOS Release 11.2(26)P. All caveats listed in this section are resolved in Cisco IOS Release 11.2(26)P6 but may be open in previous Cisco IOS releases.

- CSCed27956

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

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

This advisory is available at

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

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

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

- CSCed38527

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

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

This advisory is available at

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

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

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

Resolved Caveats—Cisco IOS Release 11.2(26)P4

Cisco IOS Release 11.2(26)P4 is a rebuild of Cisco IOS Release 11.2(26)P. All caveats listed in this section are resolved in Cisco IOS Release 11.2(26)P4 but may be open in previous Cisco IOS releases.

- CSCdw78210

Related to fixes in CSCdw65903 and outlined in:

<http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml>.

This defect may be seen when “debug snmp packets” is turned on and can result in tracebacks.

Resolved Caveats—Cisco IOS Release 11.2(26)P3

Cisco IOS Release 11.2(26)P3 is a rebuild of Cisco IOS Release 11.2(26)P. All caveats listed in this section are resolved in Cisco IOS Release 11.2(26)P3 but may be open in previous Cisco IOS releases.

- CSCdw65903

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

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

Resolved Caveats—Cisco IOS Release 11.2(26)P2

Cisco IOS Release 11.2(26)P2 is a rebuild of Cisco IOS Release 11.2(26)P. All caveats listed in this section are resolved in Cisco IOS Release 11.2(26)P2 but may be open in previous Cisco IOS releases.

- CSCdp58360
IP packets with an IP length field that is bigger than the physical size are not dropped.
Workaround: Disable Cisco Express Forwarding (CEF) switching on the input interface.
- CSCdt79947
A Border Gateway Protocol (BGP) UPDATE contains Network Layer Reachability Information (NLRI) and attributes that describe the path to the destination. An unrecognized transitive attribute can cause failures in Cisco IOS routers, ranging from a crash upon receipt of the unrecognized transitive attribute, to a later failure upon attempt to clear the unrecognized transitive attribute. Specific but common configurations are affected, and described below. The failure was discovered because of a malfunction in the BGP implementation of another vendor. There is no workaround. Affected customers are urged to upgrade to fixed code.

This vulnerability has been assigned Cisco bug ID CSCdt79947.

The complete text of this advisory is located at:
<http://www.cisco.com/warp/public/707/ios-bgp-attr-corruption-pub.shtml>
- CSCdu06400
With Cisco IOS Release 11.2(19) to 11.2(26), the Fiber Distributed Data Interface (FDDI) may never receive the reset of the address filter when the status of the Hot Standby Router Protocol (HSRP) changes from Active to Standby. This may lead to duplicate packets.

Workaround: Configure the **standby use-bia** command, or issue the **shut** command followed by the **no shut** command on the interface.
- 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 11.2(26)P

This section describes possibly unexpected behavior by Release 11.2(26)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(26)P.

Basic System Services

- CSCdj14601
When hardware compression is enabled, packets are normally fast-switched. If you disable fast switching and then enable fast switching again, fast switching remains disabled.

Workaround: Reconfigure hardware compression by entering the **no compression** command followed by the **compression stac** command.
- CSCdt00950
A Cisco 7200 router that is running Cisco IOS Release 11.2(18)P may be restarted by a bus error at PC 0x606FFF8C, address 0xC. There is no workaround.

Interfaces and Bridging

- CSCdm46655

A Cisco 7200 series router that is running Cisco IOS Release 11.1(22)CC or 12.0(9) with a port adapter (PA-F) HW rev 1.13 or 1.14 may stop transmitting packets on the FDDI interface. Packet traffic may decrease or be dropped on the interface.

Workaround: Disable and reenable the FDDI interface.

- CSCdt59139

A Cisco 7513 router with a Route Switch Processor 2 (RSP2) that is running Cisco IOS Release 11.2(17)P may display the following error message when it is used with a second generation Model 40 Versatile Interface Processor (VIP2-40) connected with a Single-port Fast Ethernet 100BASE-TX port adapter (PA-FE-TX).

```
Feb 25 04:00:09: %RSP-3-RESTART: interface FastEthernet1/0/0, output stuck
```

There is no workaround.

LAT

- CSCdt92546

A Cisco 3640 access server may not detect dynamic local area transport (LAT) service ratings advertised by dual network interface cards (NICs) installed on a LAT server that is situated on a common LAN.

Workaround: Disconnect one of the two NICs on the LAT server.

Miscellaneous

- CSCdj68910

If simultaneous accesses to NVRAM occur, the two accesses might show different sessions within the same Cisco router. For example, one session might attempt to issue the **show configuration** command and pause at the More prompt while the other session issues the **write memory** command. The problem is unlikely to occur during normal router usage. There is no workaround.

- CSCdj71794

A Cisco 3640 router may reload with a bus error when you perform direct Telnet sessions to the asynchronous ports. There is no workaround.

- CSCdm40223

A Cisco 7200 series router may exhibit bus errors, tracebacks, and spurious memory access. There is no workaround.

- CSCdt38731

A Cisco 7500 series router may reload with a bus error when crypto functions are used. There is no workaround.

Novell IPX, XNS, and Apollo Domain

- CSCdp70631

The Internetwork Packet Exchange (IPX) fast-switching cache may be invalidated by a number of external (non-IPX) related events, including an interface state change. When an external event calls for a cache invalidation, the entire cache table is invalidated. This event causes the next packet to each destination to be process-switched, possibly causing extra overhead. Ideally, IPX invalidates only entries for an interface that experience an interface state change. IP fast switching does something similar. There is no workaround.

Wide-Area Networking

- CSCdm23434

A Cisco 700 series router (Version 4.1(2)) makes an ISDN call to a Cisco 3640 router that is running Cisco IOS Release 11.2(16)P, and the Cisco 3640 has a compression module card. After a successful negotiation, subsequent PPP negotiations are unsuccessful, and the Cisco 3640 sends Combinet Proprietary Protocol (CPP) packets with wrong sequence numbers, resulting in ping failures.

Workaround: Enable PPP multilink, or remove the Compression Service Adapter (CSA) module from the Cisco 3640.

Resolved Caveats—Cisco IOS Release 11.2(26)P

This section describes possibly unexpected behavior by Release 11.2(26)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including 11.2(26)P. For additional caveats applicable to Release 11.2(26)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(26)P.

Miscellaneous

- CSCdr10521

Cisco routers that are running Cisco IOS Release 11.2 may lose the ability to create encrypted connections under the following conditions:

- The router attempts to establish two encrypted connections simultaneously.
- Both crypto maps specify access control lists (ACLs) that specify **ANY ANY** for the IP addresses.

There is no workaround.

Resolved Caveats—Cisco IOS Release 11.2(25a)P

Cisco IOS Release 11.2(25a)P is a rebuild Release for Cisco IOS Release 11.2(25)P. The caveats in this section are resolved in Cisco IOS Release 11.2(25a)P but may be open in previous Cisco IOS Releases.

- CSCdp11863

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

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

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

In lieu of a software upgrade, a workaround can be applied to certain IOS releases by disabling the ILMI community or “*ilmi” view and applying an access list to prevent unauthorized access to SNMP. Any affected system, regardless of software release, may be protected by filtering SNMP traffic at a network perimeter or on individual devices.

This notice will be posted at:

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

- CSCdr54230

A Border Gateway Protocol (BGP) UPDATE contains Network Layer Reachability Information (NLRI) and attributes that describe the path to the destination. Each path attribute is a type, length, value (TLV) object.

The type is a two-octet field that includes the attribute flags and the type code. The fourth high-order bit (bit 3) of the attribute flags is the Extended Length bit. It defines whether the attribute length is one octet (if set to 0) or two octets (if set to 1). The extended length bit is used only if the length of the attribute value is greater than 255 octets.

The AS_PATH (type code 2) is represented by a series of TLVs (or path segments). The path segment type indicates whether the content is an AS_SET or AS_SEQUENCE. The path segment length indicates the number of autonomous systems (ASes) in the segment. The path segment value contains the list of ASes (each AS is represented by two octets).

The total length of the attribute depends on the number of path segments and the number of ASes in them. For example, if the AS_PATH contains only an AS_SEQUENCE, then the maximum number of ASes (without having to use the extended length bit) is 126 [= (255-2)/2]. If the UPDATE is propagated across an AS boundary, then the local Abstract Syntax Notation (ASN) must be appended and the extended length bit used.

The caveat was caused by the mishandling of the operation during which the length of the attribute was truncated to only one octet. Because of the internal operation of the code, the receiving border router would not be affected, but its iBGP peers would detect the mismatch and issue a NOTIFICATION message (update malformed) to reset their session.

The average maximum AS_PATH length in the Internet is between 15 and 20 ASes, so there is no need to use the extended length. The failure was discovered because of a malfunction in the BGP implementation of another vendor. There is no workaround.

Resolved Caveats—11.2(25)P

This section describes possibly unexpected behavior by Release 11.2(25)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(25)P. For additional caveats applicable to Release 11.2(25)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(25)P.

- CSCdr19958

Bridged traffic running between Frame Relay and ATM connections may experience problems.

Workaround: Remove and then add the data-link connection identifier (DLCI) statement for bridged traffic to go across.

Resolved Caveats—11.2(24)P

This section describes possibly unexpected behavior by Release 11.2(24)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(24)P. For additional caveats applicable to Release 11.2(24)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(24)P.

Miscellaneous

- CSCdr10521

A Cisco router that is running Cisco IOS Release 11.2 may lose the ability to create encrypted connections under the following conditions:

- The router attempts to establish two encrypted connections simultaneously.
- Both crypto maps specify access control lists (ACLs) that specify “ANY ANY” for the IP addresses.

There is no workaround.

Resolved Caveats—11.2(23)P

This section describes possibly unexpected behavior by Release 11.2(23)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(23)P. For additional caveats applicable to Release 11.2(23)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(23)P.

IBM Connectivity

- CSCdp13665

A Cisco router that is running Cisco IOS Release 11.2 P and is configured with data-link switching plus (DLSw+) might reload and report an address of 0xD0D0D0D0 when IP connectivity issues cause Transmission Control Protocol (TCP) peers to ‘bounce.’ There is no workaround.

Interfaces and Bridging

- CSCdk83695

The “interface keep alive” option on a Fast Ethernet interface might become disabled if there is a link down event. There is no workaround.

IP Routing Protocols

- CSCdp10498

Fast switching might fail with packets larger than 1500 bytes when Network Address Translation (NAT) is enabled, even if the router is configured so that the packet is not translated using NAT.

Workaround: Disable NAT, or disable fast switching.

Resolved Caveats—11.2(22)P

This section describes possibly unexpected behavior by Release 11.2(22)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(22)P. For additional caveats applicable to Release 11.2(22)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(22)P.

IBM Connectivity

- CSCdp13665

A Cisco router that is running Cisco IOS Release 11.2 P and is configured with data-link switching plus (DLSw+) might reload and report an address of 0xD0D0D0D0 when IP connectivity issues cause Transmission Control Protocol (TCP) peers to “bounce.” There is no workaround.

IP Routing Protocols

- CSCdp10498

The fast switching of packets greater than 1500 bytes in size might fail on a Cisco router when you enable Network Address Translation (NAT), even when the router configuration does not translate the packet through NAT.

Workaround: Disable fast switching or NAT.

Resolved Caveats—11.2(21)P

This section describes possibly unexpected behavior by Release 11.2(21)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(21)P. For additional caveats applicable to Release 11.2(21)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(21)P.

DECnet

- CSCdp21639

If a Cisco router that is running a release earlier than Cisco IOS Release 11.3 and is using the DECnet Phase IV routing protocol, the DECnet network might experience loops or the incorrect selection of routes for periods of time up to the value entered with the **decnet routing-timer** command. When a network link goes up or down, one of the routers attached to that link might start sending DECnet traffic down the wrong route. You can enter the **show decnet traffic** command to show the number of messages that have been discarded with the “too many visits” count. If you enter the **show decnet route** configuration command, you can check the routes selected by the router.

Workaround: Reduce the time in the **decnet routing-timer seconds** command to reduce the time taken for the network to converge.

Interfaces and Bridging

- CSCdk83695

The “interface keep alive” option on a Fast Ethernet interface might become disabled if there is a link down event. There is no workaround.

IP Routing Protocols

- CSCdp10498

Fast switching might fail with packets larger than 1500 bytes when Network Address Translation (NAT) is enabled, even if the router is configured so that the packet is not translated using NAT.

Workaround: Disable NAT, or disable fast switching.

Resolved Caveats—11.2(20)P

This section describes possibly unexpected behavior by Release 11.2(20)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(20)P. For additional caveats applicable to Release 11.2(20)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(20)P.

Access Server

- CSCdm61555

Firmware for a 56-Kbps Microcom modem does not download after a power cycle.

Workaround: Reload your Cisco AS5200 access server manually from the command prompt. Or, download the firmware for modems manually. Or, upgrade to Cisco IOS Release 11.3, Release 12.0, or later releases.

Basic System Services

- CSCdm78804

If you are running a Cisco IOS Release 11.2 P image on a platform with MIPS R4700 and R4600 chips (including all RSP-based platforms), you might experience problems when you send a RS232 BREAK signal over a serial line. The system might reload and drop to the ROM monitor prompt rather than restart the running Cisco IOS. In addition, a malloc failure might appear at the interrupt level. There is no workaround.

Interfaces and Bridging

- CSCdm77025

Running Link Access Procedure, Balanced (LAPB) under a heavy traffic load might cause frames to get lost within the router, which results in REJECTS, backup of output queue, and output drops. There is no workaround.

IP Routing Protocols

- CSCdm71215

If the bandwidth value of serial 0/0 is set to 768 on a Cisco 3640 series router, it translates to a default Open Shortest Path First (OSPF) cost of 130, which prevents the **ip ospf** command from working properly.

Workaround: If the bandwidth value of serial 0/0 has no other use than the sum of the bandwidth of the subinterface, change the value to 760 or 770, which translates to OSPF cost 131 or 129.

Miscellaneous

- CSCdm89349

A Cisco 3600 series router that is running Cisco IOS Release 11.2 P does not recognize DSU-56K daughter cards. If you enter the **show diag** command, you will receive an “unknown daughter card” message, but this condition does not affect the functionality of the card. There is no workaround.

- CSCdm92277

An intermittent hardware problem on Route Switch Modules (RSMs) might cause the interface processor that connects to the Catalyst 5000 backplane to fail with the following error message:

```
%C5IP-0-MSG: slot0 %DB-0-FATAL_ERROR: Fatal error (code=34) status=0x0 cause=0x8020  
epc=0x80029974
```

When this occurs, the RSM has to reload the C5IP microcode, which causes all VLAN interfaces to go down for 30 to 90 seconds, with no packets being forwarded during this time. There is no workaround.

Resolved Caveats—11.2(19)P

This section describes possibly unexpected behavior by Release 11.2(19)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(19)P. For additional caveats applicable to Release 11.2(19)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(19)P.

Interfaces and Bridging

- CSCdm15864

A FDDI port adapter does not filter out unwanted multicast packets. There is no workaround.

Miscellaneous

- CSCdk74692

A Cisco 1605R series router that is running Cisco IOS Release 11.2(15a)P might allow excess User Datagram Protocol (UDP) packets to be sent inside a firewall. If the **ip inspect max-incomplete high** command is set to 10 half-open sessions, you can send more than 10 UDP packets inside the firewall, and they are not denied. There is no workaround.

Wide-Area Networking

- CSCdk80519
A Versatile Interface Processor (VIP) might experience a software-forced reload followed by a Route Switch Processor (RSP) reload. There is no workaround.

Resolved Caveats—11.2(18)P

This section describes possibly unexpected behavior by Release 11.2(18)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(18)P. For additional caveats applicable to Release 11.2(18)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(18)P.

Interfaces and Bridging

- CSCdk66951
When you configure a new E1 interface on a port adapter in a Cisco system that is based on the Versatile Interface Processor (VIP2) card, all active E1 interfaces might go down. This condition occurs even when the E1 interfaces are on separate VIP2s. This event occurs when you configure **timeslot** *start-slot–stop-slot* on the controller and **encapsulation** *encapsulation-type* on the interface. There is no workaround.

Miscellaneous

- CSCdj20961
Hot Standby Router Protocol (HSRP) and Protocol Independent Multicast (PIM) might not work together on Fast Ethernet interfaces that use the DEC211140 chipset. There is no problem if the CyBus chipset is used.
Workaround: Manually enable HSRP first and then PIM. You lose this capability if you reload the router because PIM is configured before HSRP by default.
- CSCdk68700
Encryption over dialer profiles might cause a Cisco router to reload when fast switching is enabled. This situation results in a “get alignment fatal” error.
Workaround: Disable fast switching on the dialer profile interfaces.
- CSCdk75496
When you send a break to a reverse Telnet session using a Cisco 3640 series router, you must press the **Break** key before pressing **Enter**. There is no workaround.
- CSCdk93438
A Cisco 7500 series router Versatile Interface Processor (VIP) controller might pause indefinitely when encryption is used. The problem is intermittent. Entering the **shutdown** command followed by the **no shutdown** command does not solve the problem.
Workaround: Reload the Cisco 7500 series router.

Wide-Area Networking

- CSCdk41803

A Cisco router that is running Cisco IOS Release 11.3(5.2) and is configured for ATM LAN emulation might experience software-forced reloads with the following trace message:

```
crashdump process_suspend process_may_suspend cbus_atm_sendcmd cbus_atm_tearardown_vc  
atm_remove_vc atmsig_remove_vc
```

There is no workaround.

Resolved Caveats—11.2(17)P

This section describes possibly unexpected behavior by Release 11.2(17)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(17)P. For additional caveats applicable to Release 11.2(17)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(17)P.

Access Server

- CSCdk44928

When under heavy stress, Cisco AS5200 series access servers might display a bus error and reload. There is no workaround.

Basic System Services

- CSCdk08376

Significant numbers of subinterfaces (ATM or Frame Relay) might cause “CPU HOG” messages.

Workaround: Enter the **no snmp-server sparse-table command** to reduce the number of “CPU HOG” messages.

- CSCdk11908

A Cisco 1005 series router running Cisco IOS Release 10.3(17) might repeatedly report the following errors:

```
%ETHERNET-1-TXERR: Ethernet0: Fatal transmit error. Restarting...
```

```
%QUICC-5-COLL: Unit 0, excessive collisions. Retry limit 15 exceeded
```

Testing and replacing the hardware that is attached to the router does not solve the problem. There is no workaround.

- CSCdk33318

The Cisco 7206 series router might experience a memory leak. There is no workaround.

- CSCdk41472

A Cisco 4700-m series router that is running Cisco IOS Release 11.2(14)P and is also running traffic shaping with custom queuing might experience a situation where Generic Traffic Shaping (GTS) drops are counted as custom queueing (CQ) queue drops. There is no workaround.

IBM Connectivity

- CSCdk28549
Configuring source route translational bridging and data-link switching (DLSw) to the same bridge group at the same time might result in traceback messages and ultimately might cause the router to reload.

Workaround: Deconfigure source route translational bridging, or deconfigure the DLSw connection to the bridge group.

Interfaces and Bridging

- CSCdj85213
The primary Synchronous Digital Link Control (SDLC) interface might send out an erroneous frame causing a secondary device to send a Frame REJECT(-FRMR). There is no workaround.
- CSCdk11808
Some terminal adapters might toggle control lines during data terminal routing (DTR) pulsing. These line status changes will interrupt the PA-8T/4T+ port adapter controller and cause the Cisco IOS driver to reset the line. The DTR pulse is shortened in this condition. There is no workaround.
- CSCdk20550
The 10-Mbps full-duplex capability of the Cisco 3600 series NM-1FE-TX router in Cisco IOS Release 11.2 P does not operate properly. The speed toggles between 10 Mbps and 100 Mbps, which affects the connectivity. There is no workaround.
- CSCdk39193
When the RX or TX clock is missing, the HSSI3 code waits for the chip reset to be completed at the beginning of the code, but the chip reset is only done at booting or online insertion and removal. When both TX and RX clocks are present, bit 0 of STATUS6 is set, and a microcode can proceed with no difficulties. The microcode, however, sticks at PC=0 when the system possesses only one clock. The system will continue to function regardless of this reset status. There is no workaround.
- CSCdk53401
When you netboot a Cisco 3640 series router over the Fast Ethernet port, the Cisco IOS software proceeds with an interactive setup without trying to load configurations from the network. This situation is caused by an autonegotiation race condition in which the Fast Ethernet port momentarily appears to be in a down state. There is no workaround.

IP Routing Protocols

- CSCdj49045
The C programming language print function “Printf” might suspend the current process if the calling process inhibits a process context switch to protect its processing. This condition will cause a Cisco router to reload. There is no workaround.
- CSCdk20424
For commands without ACKs on NEC V.110 modems, the “notify_tx_complete” message is treated as an ACK, and an appropriate message goes to the sender. This feature might not work in the older revision V.110 from NEC. There is no workaround.

- CSCdk23751

If there is no router at the end of a connection, and you attempt to encrypt to the missing side, problems might occur in the connection setup code. There is no workaround.

- CSCdk34128

On an M4T or M8T adapter, a Cisco router might experience a depletion in packet memory after generating enough network traffic to saturate a serial interface. The only method of recovering the memory is reloading the router. There is no workaround.

Miscellaneous

- CSCdk47147

If you enter the **async mode dedicated** command or the **async mode interactive** command on a Cisco AS5200 or Cisco AS5300 access server with a Modem ISDN channel aggregation (MICA) modem, the router might reload with a bus error and exhibit a “%ALIGN-1-FATAL” log message. This situation occurs when a large number of PPP calls are connecting and disconnecting. There is no workaround.

- CSCdk53807

An encryption service adapter does not work with pregeneration.

Workaround: Disable pregeneration functionality by entering the **no crypto pregen-dh-pairs** command.

- CSCdk64463

When bridging is configured on a Route Switch Module (RSM) VLAN interface that runs Cisco IOS Release 11.2 P or Cisco IOS Release 11.3, NetFlow or optimum switching does not occur. When bridging is configured on a Route Switch Module (RSM) VLAN interface that runs Cisco IOS Release 12.0, Cisco express forwarding (CEF) switching does not occur. IP packets are processed by fast switching instead of flow/optimum/CEF switching, causing a significant decrease in the IP packet forwarding rate. The NetFlow Collector might also fail. There is no workaround.

Wide-Area Networking

- CSCdj81263

When IP fast switching is enabled on a Cisco 1600 series router that has a Basic Rate Interface (BRI) or BRIs, the router might reload if the ISDN connection is being brought up and down repeatedly, and the **clear ip cache** command is invoked repeatedly while the connection is being disconnected. There is no workaround.

Resolved Caveats—11.2(16)P

This section describes possibly unexpected behavior by Release 11.2(16)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(16)P. For additional caveats applicable to Release 11.2(16)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(16)P.

Basic System Services

- CSCdj20725
RSP-based platforms might reload at `rsp_fs_free_memd_pack` because packets need to be fragmented that have the `dontfrag` bit set in the IP header.
This issue can be seen in several different ways, including bus errors at `XX200001`, bus errors at `3DFEFEFEF`, and process stack corruption due to the overflowing process-switched packet queues (process stacks). There is no workaround.
- CSCdj22469
An IP packet with Don't Fragment (DF) set might be fragmented and switched in the optimum switching path instead of being dropped and replied with an ICMP packet.
Workaround: Disable optimum switching and let the process level handle the IP fragmentation.
- CSCdk08985
Changing encapsulations on a PRI interface while there are users connected might cause a Cisco router to reload.
Workaround: Shut down the PRI interface, and then change the encapsulation.

Interfaces and Bridging

- CSCdj94063
XNS over LANE might not work in fast-switching mode on Cisco 7200 series routers.
Workaround: Use process switching.

Miscellaneous

- CSCdj88250
Under rare circumstances, the Modem ISDN channel aggregation (MICA) modems on a Cisco 3600 series router might get stuck in terminating state and possibly be marked "Bad." In this situation, the modem becomes unusable until the router is reloaded. This problem appears to be aggravated when using T1 CAS interfaces for the digital modems. There is no workaround.
- CSCdk16022
When switching from the software engine to the hardware engine and back again, and then applying the crypto map, packets might not get encrypted or decrypted. There is no workaround.
- CSCdk22184
After a connection is set up with the hardware engine, switching to the software engine might result in an error that indicates that the HMA handle could not be found. There is no workaround.

Wide-Area Networking

- CSCdj77099

When there are open channels on a PRI for a Cisco AS5200 access server that is running Cisco IOS Release 11.3(1), some incoming voice calls might be rejected with a “No free channels: CALL_INCOMING, Voice: ERROR” message. This occurs with incoming ISDN voice calls only. There is no workaround.

- CSCdk22842

A Cisco router that is running Cisco IOS Release 11.2P and has a PRI interface that is only used for dial-in ISDN access might experience problems with inbound calls if Dialer Caller is used with Dialer Profiles to screen the inbound calls. When a call is received by the router with the correct bearer capability, the call is rejected as unbindable if the calling party information is from any source not explicitly listed in the dialer profiles, or there is no dialer caller information. The next inbound call attempt will then be released with the cause message of “Requested channel not available.” The call control blocks (CCBs) stay allocated for these rejected calls, and the PRI appears hung, which means that dial-in calls cannot be received.

Workaround: Reset the PRI with the **shutdown** command. Wait 30 seconds, and then enter the **no shutdown** command.

Resolved Caveats—11.2(15)P

This section describes possibly unexpected behavior by Release 11.2(15)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(15)P. For additional caveats applicable to Release 11.2(15)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(15)P.

Basic System Services

- CSCdj84652

Any interface that uses encryption service adapter (ESA) service should have the maximum transmission unit (MTU) configured to no larger than 16 KB because the ESA does not support packets over 16 KB. There is no workaround.

- CSCdk08985

Changing encapsulation on a PRI while users are connected might cause the router to reload.

Workaround: Shut down the PRI first, then change the encapsulation.

IBM Connectivity

- CSCdk05874

A downstream physical unit (DSPU) cannot be configured under a VLAN interface. There is no workaround.

Interfaces and Bridging

- CSCdk04111
Transparent bridging IP over FDDI might fail. There is no workaround.
- CSCdk08386
A Cisco 7200 series router that is running Cisco IOS Release 11.2(13)P1 with fast switching enabled cannot handle a small packet, which is less than 46 bytes for IP datagram size.
Workaround: Enter the **no ip route-cache** command on the Bridge Group Virtual Interface (BVI). Fast switching works with any data length.

LLC Type 2

- CSCdk07546
Retransmitted frames by an Advanced Peer-to-Peer Networking (APPN) router using remote source-route bridging are truncated. There is no workaround.

Miscellaneous

- CSCdj80895
If you are using the Cisco IOS firewall feature with context-based access control to inspect TCP, the router might reset if fast switching is enabled. There is no workaround.
- CSCdj93566
When using encryption with the backup feature and the line protocol, and the primary connection goes down, the router might not clear existing crypto connections on the primary path, and crypto connections using the backup circuit fail to establish correctly. According to the output generated by the **show crypt eng conn act command**, the router behaves as if the crypto connections are running correctly over the down interface. This behavior persists until the primary path is restored. This problem does not occur if the primary path goes down physically. There is no workaround.
- CSCdk07174
Routers that are configured to host Cisco Cache Engines that are using the Web Cache Control Protocol (WCCP) might treat any host that sends them valid WCCP data as a Cache Engine, regardless of whether that host is actually a legitimate cache service provider. This condition can be exploited to divert HTTP traffic to unauthorized users.
Workaround: Use input access lists to prevent WCCP traffic sent by unauthorized hosts from reaching the router. WCCP uses User Datagram Protocol (UDP) on port 2048.
- CSCdk12480
A VIP crypto engine might not successfully negotiate a crypto connection with a crypto peer if traffic that needs to be encrypted or decrypted by the VIP is received at an initialization time, such as after a reload or an online insertion and removal (OIR). After the VIP has reinitialized, entering **show crypto connection** shows an ID of "0." However, entering **show crypto map** will show a negative connection ID.
Workaround: Clear the ID manually by entering the **clear cryp connection connection_ID vip_slot # command**. The router will display an error message, but it will successfully negotiate a crypto connection.

Wide-Area Networking

- CSCdj67875
When configuring integrated routing and bridging (IRB) to bridge over a serial interface with High-Level Data Link Control (HDLC) or Frame Relay encapsulation, AppleTalk might not work properly. AppleTalk pings fail, and zone information is not transferred. There is no workaround.
- CSCdk05107
A Cisco router might display an “unknown sub-interface type 0x2” message when Frame Relay subinterfaces are configured on Frame Relay Network-to-Network Interface (NNI). This display might cause a system reload or a kernel error message, such as “SYS-2-NOBLOCK messages.” There is no workaround.

Resolved Caveats—11.2(14)P

This section describes possibly unexpected behavior by Release 11.2(14)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(14)P. For additional caveats applicable to Release 11.2(14)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(14)P.

Access Server

- CSCdj81150
Incoming calls to a Cisco AS5200 or Cisco AS5300 access server that has a T1/E1 controller running Robbed Bit Signalling type “E&M feature group D” might fail because of the short delay between winks. Outgoing calls are not affected. There is no workaround.
- CSCdj91500
A Cisco AS5300 access server that is using E1/R2 signalling, channel associated signalling (CAS) 3, and analog modems might reload when it receives incoming analog calls. This problem can occur with Cisco IOS Release 11.2(11)P, Cisco IOS Release 11.2(12)P, and Cisco IOS Release 11.3(2)T.
Workaround: Configure **dnis-digits x** under **cas-custom**, where the integer “x” is the number of DNIS digits expected from the CO switch. Range: $0 < x < 66$.

Basic System Services

- CSCdj72511
If you are upgrading to Cisco IOS Release 11.3(0.8), Cisco IOS Release 11.2(9.2), Cisco IOS Release 11.3(0.8)T, Cisco IOS Release 11.2(9.2)P, Cisco IOS Release 11.2(9.2)BC, or Cisco IOS Release 11.3(0.8)MA, and you are using the TACACS+ update accounting packet to track assigned user IP addresses, you must configure the **aaa accounting update newinfo command** before the update accounting packet can be generated in the newer release. There is no workaround.

EXEC and Configuration Parser

- CSCdj94422

A problem occurs when a client that is configured with 7 data bits and even parity dials into an asynchronous interface that is configured for 8 data bits, no parity, and autoselect. The autoselect process does not recognize a carriage return and does not start an EXEC session. The carriage return comes into the router as hex 0x8D. There is no workaround.

Interfaces and Bridging

- CSCdj69939

If CRC32 is configured between two Packet OC-3 Interface Processors (POSIPs) with hardware revision 1.4 or below, upgrading one POSIP to hardware revision 1.5 or above may lead to packets that are 2 bytes too short or too long as reported by the **debug ip packet** command. In this situation, only a router reload solves the problem.

Workaround: Set CRC16 on both ends before upgrading the POSIP.

IP Routing Protocols

- CSCdj59706

Enhanced Interior Gateway Routing Protocol (EIGRP) might not take directly connected host routes into the topology table and redistribute them to other routers. There is no workaround.

Wide-Area Networking

- CSCdj33387

In some cases, outgoing calls where the call ID is 0x8000-0xffff are not properly released. The call ID assigned to a new, outgoing call is not checked against outstanding calls, and the call ID is incorrectly assigned when a call already exists with that call ID. The result is that the incorrect call is released when a call with the duplicate call ID is disconnected. There is no workaround.

- CSCdj90223

When a Cisco router creates and releases multiple Frame Relay switched virtual circuits, some of the switched virtual circuits might not be released correctly. This problem does not happen when only one switched virtual circuit is created and released. There is no workaround.

Resolved Caveats—11.2(13)P

This section describes possibly unexpected behavior by Release 11.2(13)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(13)P. For additional caveats applicable to Release 11.2(13)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(13)P.

Access Server

- CSCdj73991

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

Workaround: Remove and re-enter the **cas-group** command on the controllers.

IBM Connectivity

- CSCdj80779

The **ip helper-address** command might not work on a FDDI interface on a Cisco 7200 series router if the User Datagram Protocol (UDP) frame contains a Routing Information Field (RIF) source, and source-route bridging (SRB) is enabled on the interface. There is no workaround.

- CSCdj82340

A Cisco 7513 series router that is running remote source-route bridging (SRB) with a large number of peers might reload on start-up if the traffic load is high.

Workaround: Remove the peers, and then reinsert them one by one. This solution allows the router to assume the load gradually and continue functioning.

Interfaces and Bridging

- CSCdj76918

A Cisco router might reload if there is an sw56k/ft1 CSU/DSU in slot 1, and slot 0 is either empty or has a module other than an sw56k/ft1 CSU/DSU.

Workaround: Insert the sw56k/ft1 CSU/DSU in slot 0 of 2524.

- CSCdj78877

A Cisco 7200 series router Ethernet interface that is configured for PIM might not receive multicast packets if the interface has not joined that group. As a result, the router does not receive Internet Group Management Protocol (IGMP) v2 group membership reports (sent by members to the group address) if the router is not a member of the group.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the interface after rebooting.

IP Routing Protocols

- CSCdj67271

A Cisco router that is supporting Fast Ethernet that is configured with Inter-Switch Link (ISL) encapsulation will place an entry in its Address Resolution Protocol (ARP) table if a client in one VLAN is incorrectly configured with an IP address in the subnet assigned to another VLAN that is supported within that trunked interface. There is no workaround.

Miscellaneous

- CSCdj80643
A Cisco 3640 router with a six-modem MICA SIMM might reload during bootup unless the six-modem MICA SIMM is installed in Bank 0 of the Digital Modem Network Module. There is no workaround.
- CSCdj81104
When Route Switch Modules (RSMs) are configured to use DEC spanning tree protocol on a bridge group, the RSMs might not block an interface that should be blocked, creating a bridging loop. There is no workaround.
- CSCdj82169
Boardware on a Cisco AS5300 access server might slice the data incorrectly. The problem occurs at random on a per-line basis across all boards and ports running Cisco IOS Release 11.2(10a)P1 with 2.0.1.7 portware, 1.3.3.5 boardware, and revision A0 on the Amazon board. You will see trashed data in and out of a bad line. If you are running PPP over the modem link, the symptom will be input errors. If you are running a dialin EXEC session, the characters entered might be echoed out of order. If you are running a reverse Telnet session, lines of data sent from the modem to the telnet session might appear out of order.
Workaround: Powercycle the Cisco AS5300.
- CSCdj84770
If the number Teralink systems that are configured but not connected reaches four, the Cisco 7500 series router signalling software might not respond to requests sent from connected Teralink systems. If you try to remove cable configuration entries, those entries will still show up with a “show cable channel” message. If new modems come online, the router will not display those modems, and exhibit a “show cable modem” message. Modems will stay in “disconnected” state within the Teralink indefinitely. If modems are disconnected, entries will still show up with the **show cable modem** command. There is no workaround.

Resolved Caveats—11.2(12)P

This section describes possibly unexpected behavior by Release 11.2(12)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(12)P. For additional caveats applicable to Release 11.2(12)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(12)P.

Basic System Services

- CSCdj12951

Better reload information is needed to debug data/stack corruption reloads. The solution is to write reload information to default to bootflash:crashinfo in RSP and flash:crashinfo in RP. A series of **test crash** command selections are used to control and change the crashinfo collection mechanism. The reload information contains up to 32 KB in RSP and up to 20 KB in RP of error message log plus command history including configuration commands that the user enters. The reload information also contains up to 32 KB on RSP and 20 KB on RP for all the following information:

- crash stack trace
- crash context
- stack dump at crash
- dump memory for each register containing “valid” RAM address
- error message display on invalid length of bcopy
- two commands to “test crash”

The **show stack** command displays (“cat” as in UNIX) the bootflash:crashinfo file if there was a crash. The user can also use the command **copy flash tftp** to dump the ASCII file bootflash/flash:crashinfo to a server.

The size is 16 KB of errmsg/command, plus up to 16 KB of memory dump and other crash information. There is one 16-KB DRAM declared for this crash information collection mechanism. Only Cisco 7000 series routers and RSP are activated with new crashinfo mechanism and the 16 KB. The Cisco 4500 router and other devices will see no difference.

Interfaces and Bridging

- CSCdj48322

When using E1 or T1 port adapters in channelized mode, the open timeslots should be assigned to an interface while the interface is shut down. If not, the router might affect other used timeslots and degrade their performance. There is no workaround.

- CSCdj29724

After you unplug the cable and then plug it back in again, the ATM interface might ignore packets at a low packet rate.

Workaround: Enter the **shutdown** command followed by the **no shutdown** command to reinitialize the interface.

- CSCdj64480

A Cisco router might reload with a bus error when you configure source-route translational bridging. There is no workaround.

- CSCdj54162

The PA-8T port adapters on VIP2-40 interfaces flap intermittently when you enable hardware compression. This problem does not occur when compression is disabled. Note that hardware compression does not work with High-Level Data Link Control (HDLC) encapsulation in Cisco IOS Release 11.2(9)P, so PPP encapsulation is used in this case. The eight-port serial port adapter might have intermittently flapping interfaces when used with a hardware compression port adapter.

Workaround: Set the serial restart-delay to the maximum value.

Miscellaneous

- CSCdj80853

The IOS recovery actions for a Cisco Catalyst 5000 Route Switch Module (RSM) experiencing controller errors might cause network outages that last for a few seconds. The output from the **show controller c5ip** command can tell you if the controller has experienced these errors. For example, the example below reveals that this particular controller has detected 1387265 CRC errors and 1213882 DMA synchronization errors on Channel 0:

```
DMA Channel 0 (status ok) Received 11525644K packets, 8940433M bytes One minute rate,
183331545 bits/s, 28869 packets/s Ten minute rate, 183690578 bits/s, 28899 packets/s
Dropped 285660 packets 285472 ignore, 0 line-down, 0 runt, 0 giant, 188 unicast-flood
Last drop (0xA1F446D), vlan 109, length 1295, rsm-discrim 0, result-bus 0xD Error
counts, 1387265 crc, 0 index, 0 dmac-length, 1213882 dmac-synch Transmitted 224504
packets, 15939644 bytes One minute rate, 313 bits/s, 1 packets/s Ten minute rate, 313
bits/s, 1 packets/s
```

```
DMA Channel 1 (status ok) Received 5473296K packets, 4209913M bytes One minute rate,
86473427 bits/s, 13724 packets/s Ten minute rate, 86453598 bits/s, 13719 packets/s
Dropped 55916 packets 0 ignore, 0 line-down, 0 runt, 0 giant, 55916 unicast-flood Last
drop (0x814001), vlan 1, length 64, rsm-discrim 0, result-bus 0x5 Error counts, 0 crc,
0 index, 0 dmac-length, 0 dmac-synch Transmitted 198226401 packets, 153955044K bytes
One minute rate, 402 bits/s, 1 packets/s Ten minute rate, 404 bits/s, 1 packets/s.
```

There is no workaround.

Wide-Area Networking

- CSCdj48055

PRI might pause indefinitely or return a busy signal even though not all channels are in use. This condition is usually accompanied by the following console messages:

```
ISDN Se9/0/1:23: Error: CCB run away: 0x61D97560:
ISDN Se9/0/1:23: Error: CCB run away: 0x61C494F8:
ISDN Se9/0/1:23: Error: CCB run away: 0x61C494F8:
```

A call control block (CCB) is an internal structure. You should only have one per call and B channel. For an example, interface serial 9/0/1 has 60 CCBs.

Workaround: Reset the controller manually entering the **shut** command followed by the **no shutdown** command for the interface serial0:XX or by reloading the router.

- CSCdj67880

A Cisco 7200 series router might reload at the atmSig_input routine under normal operations. There is no workaround.

Resolved Caveats—11.2(11)P

This section describes possibly unexpected behavior by Release 11.2(11)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(11)P. For additional caveats applicable to Release 11.2(11)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(11)P.

Basic System Services

- CSCdj26122

If you have enabled optimum or NetFlow switching, the input counters from the **show frame-relay pvc** command are not correctly updated. There is no workaround.

- CSCdj61798

A Cisco AS5300 access server will allow the creation of more than five vtys only in the enterprise image. There is no workaround.

IBM Connectivity

- CSCdj48508

If you configure source-route bridging on the FDDI interface of a Cisco 7200 series router that is running Cisco IOS Release 11.2, IP routing protocols on the same FDDI might stop working. There is no workaround.

Interfaces and Bridging

- CSCdj49030

A PA-4RFDX port adapter with a VIP2/20 might experience problems with interfaces initializing. The output queue on the interface might fill up (40/40).

Workaround: Use the recommended VIP2/40 for the 4R full-duplex card. This does not apply to regular 4R.

IP Routing Protocols

- CSCdj62042
In Cisco 7500 series routers, packet transmission failure is expected if the inbound Switched Multimegabit Data Service (SMDS) encapsulated packet size is greater than the maximum transmission unit (MTU) of outbound media. This problem will occur only if the optimum switching is turned off by entering the **no ip route-cache opt** command, and if fast switching is enabled.
Workaround: Enter the **ip route-cache optimum** command on the serial interface that has SMDS encapsulation.
- CSCdj53541
Entering the **no ipx routing** command and then enabling Enhanced IGRP with the **router eigrp** command might cause a Cisco router to reload. There is no workaround.

Resolved Caveats—11.2(10)P

This section describes possibly unexpected behavior by Release 11.2(10)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(10)P. For additional caveats applicable to Release 11.2(10)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(10)P.

Basic System Services

- CSCdj21474
If you configure an FTC trunk and an SPVC connection and then delete these configurations, a Cisco router might display a “Sparc process not responding, reloading” message the next time you configure the FTC trunk. The failure might occur after one such sequence or after a number of similar sequences of commands. This will only occur if the operator has yet not saved the configuration.
Workaround: Update the configuration changes immediately by entering the **write memory** command.
- CSCdj38964
The **copy bootflash {rcp | tftp}** and **copy {rcp | tftp}** commands are not supported in Cisco IOS Release 11.2(10)P.
Workaround: Use the **copy flash {rcp | tftp} |file-id}** command to copy from flash memory to TFTP, or RCP instead of using the **flash** keyword. Please note that this workaround does not work with the **boot flash** command.
- CSCdj45167
Periodical chunk sanity check might not check the sibling chunk list. Normal chunk operation is not affected. There is no workaround.

IBM Connectivity

- CSCdj49533
When enabling the source-route translational bridging feature, a Cisco router might run out of I/O memory because of a buffer leak in small and middle buffers.
Workaround: Disable source-route translational bridging.

Interfaces and Bridging

- CSCdj24890
The internal clock on an ATM port adapter might not initialize properly. This situation causes a loopback ping to fail because neither end is providing the clock. There is no workaround.
- CSCdj47294
Custom queueing does not work on a Cisco 7505 series router that is running Cisco IOS Release 11.1(14)CA with an RSP4 and an E1 port adapter. There is no workaround.
- CSCdj51923
The ATM port adapter on a VIP2 platform might not function properly. In this situation, the interface output gets stuck, and the interface keeps resetting. There is no workaround.

Wide-Area Networking

- CSCdj42202
Fast switching might not work properly on a Cisco 7200 series router that is running Multilink PPP on a Channelized T1/E1 ISDN PRI port adapter. Only the first packet is sent through the interface, and subsequent packets are dropped.
Workaround: Disable fast switching by entering the **no ip route-cache** command on the interface.
- CSCdj43717
A Cisco router that is configured with “isdn incoming-voice data 56” might incorrectly recognize an incoming voice call as 64K. There is no workaround.
- CSCdj46634
When an ATM port adapter is the third of the three Fast Ethernet port adapters on an NPE-150, and its receive pool is forced to operate out of DRAM, or when an ATM port adapter is running in an NPE-100, where it is designed to operate out of DRAM, packets that should be handled at the process level will end up in wrong queues. There is no workaround.
- CSCdj46914
An ATM port adapter that is connected to a Newbridge might cause the laser to shut down for two seconds after running for eight seconds. When you replace the ATM port adapter with an AIP, the laser works. There is no workaround.

Resolved Caveats—11.2(9)P

This section describes possibly unexpected behavior by Release 11.2(9)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(9)P. For additional caveats applicable to Release 11.2(9)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(9)P.

Basic System Services

- CSCdj25189
Cisco 7200 series routers do not produce a core dump for the I/O memory region in any Cisco IOS release, but you might need this information if memory corruption is suspected. There is no workaround.
- CSCdj27067
When using distributed compression (VIP software compression), if input congestion occurs where an input buffer cannot be allocated, an illegal packet might be sent to the host causing unpredictable results including “output stuck” messages that result in a CBUS reset. This has been found on a VIP with four PRI interfaces doing distributed compression.
Workaround: Disable distributed compression.
- CSCdj27391
A Cisco 3600 series router is missing the modemcap and modem auto discovery subsystems in the Service Provider subset images (c3620-p-mz and c3640-p-mz) in Cisco IOS Release 11.1 AA and Cisco IOS Release 11.2 P. Other Cisco 3600 series router images are not affected. There is no workaround.
- CSCdj27481
A Cisco router with a MIPS 4000 processor might not reply correctly to Network Time Protocol (NTP) time requests. This problem exists only in Cisco IOS Release 11.2 P. There is no workaround.
- CSCdj41427
In Cisco IOS Release 11.2 P images, traffic-shaping is not enabled in the process-switching path when FIFO queuing is active on the output interface and in the fast-switching path. Traffic shaping shapes well above CIR on interface with FIFO queuing enabled.
Workaround: Change the queuing algorithm from FIFO to fair-queue on that interface if you want to use a Release 11.2 P image, or a Release 11.2 mainline image.

IBM Connectivity

- CSCdj33360
The source-route translational bridging (SR/TLB) feature might not function correctly, and sessions through SR/TLB cannot be established. There is no workaround.
- CSCdj42984
When doing source-route bridging (SRB), specifically routed or directed frames might have 4 bytes appended to the frames.
Workaround: Disable fast switching.

Interfaces and Bridging

- CSCdj01556
A Versatile Interface Processor (VIP) with a PA-A1 port adapter might reload when configured to do distributed local switching on the same interface, for example, packets coming into the PA-A1 port adapter on one VC and going out on another VC on the same PA-A1 port adapter interface. There is no workaround.
- CSCdj25270
Call setup might fail with AIPREJCMD & AIP-3-FAILCREATEVC messages on a PA-A1 port adapter. There is no workaround.
- CSCdj28822
Mx serial port adapters (PA-4T+, PA-8T, PA-H1T, PA-H2T) might pause indefinitely and experience buffer errors and bad reference counts. There is no workaround.
- CSCdj28940
Cisco 7200 series routers do not support both integrated routing and bridging (IRB) and multicast enabled. The router might exhibit the following error message if IRB and multicast are enabled:

```
%SYS-2-BADBUFFER: Attempt to use scattered buffer as contiguous src, ptr= 60C0C3BC, pool= 60C0AC28 %ALIGN-3-CORRECT: Alignment correction made at 0x6026ADB0 reading 0x1AA0056 %ALIGN-3-CORRECT: Alignment correction made at 0x6026B078 reading 0x1AA0046
```


There is no workaround.
- CSCdj29082
The external/test port status display shown in the output from the **show cont t3** command is not reliable. Regardless of the port's real state, it might show

```
Ext1: OK, Ext2: OK, Ext3: OK, Test: OK
```


If the state of any port changes sometime after booting, then all four ports will display their actual state. If no such change happens, the display will continue to show OK, OK, OK, OK, regardless of the actual state. There is no workaround.
- CSCdj31285
A Cisco router might not respond to Address Resolution Protocols (ARPs) correctly when bridging IP on a channelized T1 interface, and Telnet sessions to and from the router will fail. There is no workaround.
- CSCdj32880
The ATM port adapter's PCI bus latency timer value is too small, which might cause some inefficiency on the PCI bus utilization on a VIP2. There is no workaround.
- CSCdj33727
Under certain circumstances, the Fast Ethernet interface on a Cisco router might stop passing traffic. Resetting the interface in this condition by entering the **shutdown** command followed by the **no shutdown** command might cause the router to reload. There is no workaround.
- CSCdj34424
When a virtual circuit creation fails because the maximum number of virtual paths are used up, it might waste the virtual circuit descriptor (VCD) being used and not recycle it. The VCD remains unusable afterwards. There is no workaround.

IP Routing Protocols

- CSCdj35044

After a Cisco 1600 series router that is running Cisco IOS Release 11.2(7.3)F with Network Address Translation reloads, the router might fail to establish a Dial on Demand connection over the asynchronous interface. The condition occurs in configurations that use Easy IP over the asynchronous interface in addition to Network Address Translation.

Workaround: Enter the **no ip nat** command followed by the **ip nat** command.

Miscellaneous

- CSCdj34609

The Cisco IOS Release 11.2(7)P RSP encryption images might reload if booted on a router which has not had the configuration setup before.

Workaround: Boot a non-encryption image. Or, boot an older encryption image to create the initial configuration.

TN3270

- CSCdj22231

International (8-bit) characters might not echo when using TN3270. There is no workaround.

Resolved Caveats—11.2(8)P

This section describes possibly unexpected behavior by Release 11.2(8)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(8)P. For additional caveats applicable to Release 11.2(8)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(8)P.

Access Server

- CSCdj19651

A Cisco AS5200 access server that is connected to a noisy line might reload with a bus error at PC 0, address 0 if there is a very high rate of channelized T1/E1 signalling transitions. There is no workaround.

- CSCdj22879

A Cisco AS5200 access server that is running Cisco IOS Release 11.2(6.4)F might exhibit the following messages during a reload:

```
*Mar 1 00:02:19.651: %CALLS_MGMT-1-CPM_Q_POOL: Cannot get memory for process watched queue entry *Mar 1 00:02:21.851: %CALLS_MGMT-1-CPM_Q_POOL: Cannot get memory for process watched queue entry *Mar 1 00:02:25.931: %CALLS_MGMT-1-CPM_Q_POOL: Cannot get memory for process watched queue entry
```

The Call Management (CM) code maintains a circular buffer from which it retrieves space for its process queue entry. Under normal operating conditions, there is enough space on this buffer to accommodate CM. However, during system start-up, if start-up tests are enabled for a modem, it might behave as if it is connecting a call. This causes messages to be sent to CM. While CM will be able to recognize that no actual call is being setup, the sheer number of messages sent by 48 modems (Brasil) in parallel could result in overflows and cause corruptions in the buffer. The manifestation of this problem is the display of the following messages during system start-up:

```
... %CALLS_MGMT-1-CPM_Q_POOL: Cannot get memory for process watched queue entry %CALLS_MGMT-1-CPM_Q_POOL: Cannot get memory for process watched queue entry %CALLS_MGMT-1-CPM_Q_POOL: Cannot get memory for process watched queue entry %CALLS_MGMT-1-CPM_Q_POOL: Cannot get memory for process watched queue entry %CALLS_MGMT-1-CPM_Q_POOL: Cannot get memory for process watched queue entry ...
```

If you are running an image which does not have the fix for this problem (CSCdj22879), the workaround would be to disable the start-up tests for the modems. This problem has been observed with Microcom modems, and at the time of this writing, Amazon modems are not yet available for testing. There is no workaround.

- CSCdj24098

A High-Speed Serial Interface (HSSI) port adapter might handle packets abnormally under high traffic conditions. Customers using 7200/HSSI PAs are strongly encouraged to upgrade to an image containing the fix for this bug. There is no workaround.

Basic System Services

- CSCdj14049

A Cisco 3640 series router might pause indefinitely while running Cisco IOS Release 11.2(8)P. There is no workaround.

- CSCdj23217

The performance of frame switching from the Ethernet interface to an FTC trunk interface is approximately 500 fps (frames per second). This condition causes severe limitation on performance. There is no workaround.

IBM Connectivity

- CSCdj23339

A Cisco router might refuse to accept the configuration of the Role or character type if you attempt to configure binary synchronous communication (BSC) on a low-speed interface of the NP-2T 16S-RS323 network interface card (NIC). There is no workaround.

Interfaces and Bridging

- CSCdj09796
When a shutdown is issued on an PA-A1 port adapter interface while it's transmitting large packets (>512 bytes) at a high rate, there is a chance that it will reload the router. Similarly, when a shutdown is done while it's receiving traffic, there is a chance it will lose some buffers. There is no workaround.
- CSCdj12144
This bug is caused by the 8T and 4T+ on the VIP could not send out a dial string. The fix was committed and it should be available at 11.1(13)CA and 11.2(8)P. Without the fix, the above synchronous interface (on VIP) can not support Dial on Demand feature. There is no workaround.
- CSCdj15944
When a Cisco 3600 series router is configured for HSRP, and pinging the standby's router real address, there are duplicated echo replies. The same when configured for MHSRP. There is no workaround.
- CSCdj18441
Under high traffic conditions the HSSI PA may handle the packets abnormally.
Customers using VIP2/HSSI PAs are strongly encouraged to upgrade to an image containing the fix for this bug. See "Field Alert: VIP2 Cisco IOS Software Release Deferrals" for image availability and additional information. There is no workaround.
- CSCdj22705
The async/sync interfaces in async. mode did not support group-async until 11.2(6.01)P. This problem was addressed by CSCdi86295 which was fixed and was put in 11.2(6.01)P in general. But for 3600 platform with 4/8 A/S Network Module in particular, the group-async command still does not work properly with the current release. It would result in losing configuration for those async/sync interfaces in async mode under group-async after reload. The work around is to avoid using the group-async command with 4/8 A/S Network Module interfaces in async. mode. Each 4/8 A/S in async. mode must be configured individually. There is no workaround.
- CSCdj23273
Compression with stac and HDLC had performance impact and encapsulation PPP didn't do any compression. There is no workaround.
- CSCdj23299
OVERVIEW: This update provides information on bug fixes for the CT3IP available in Cisco IOS Release 11.1(12)CA1. Because of these fixes, Release 11.1(12)CA1 will be the minimum release for new CT3IP orders.
PROBLEMS: 1. Problems with packet error accounting. Ignores on the CT3IP were regularly being counted as overruns. Incorrect error accounting can lead to erroneous information on network status being provided to network operations personnel.
2. Packet handling errors: In lab tests, Cisco engineers discovered a latent bug in the CT3IP that can result in abnormal packet handling under unusually severe operating conditions. While Cisco is taking preemptive action to correct this bug, Cisco does not expect this bug to manifest itself in operational networks.
Workaround: Run the CT3 above 80 Kpps on average per direction, and upgrade to Cisco IOS Release 11.1(12)CA1 available on Cisco.com now.

ISO CLNS

- CSCdj22028

When configuring “connectionless service” using the **clns** command, a Cisco 3800 series router will reload with a bus-error after entering the **clns route** command. There is no workaround.

Miscellaneous

- CSCdj16069

If you attempt to configure the **ignore-dcd** command under Cisco IOS Release 11.1(xx)AA, the command looks as though it should be there but does not work. This command applies to WIC-1T interfaces on the Cisco 3600 series. There is no workaround.

Novell IPX, XNS, and Apollo Domain

- CSCdj19117

When the Internetwork Packet Exchange (IPX) packet (incoming) is greater than 1500, it gets dropped even if the maximum transmission unit (MTU) size of the outgoing interface says that the interface should be able to handle the incoming packet.

Workaround: Update the interface data structure to reflect the any new changes to the MTU.

Wide-Area Networking

- CSCdj17845

It was found that the DRQ was becoming corrupted as a result of recursive invocation of drq_io (Interprocess Communications (IPC) packet passed to IPC code via dtq_consumer could result in a packet being returned via drq). drq_io was made safe for recursion. There is no workaround.

- CSCdj24827

With changes made for CSCdj 7845 (recursive drq_io allowed), it became possible for QE to start work on a DRQ transfer entry, only to have the kernel code later change that entry. Solution is to write transfer entry after all other data entries. There is no workaround.

Resolved Caveats—11.2(7)P

This section describes possibly unexpected behavior by Release 11.2(7)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(7)P. For additional caveats applicable to Release 11.2(7)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(7)P.

Basic System Services

- CSCdj07295

When a voice circuit is configured for SVC operation from a Cisco 3800 series router to a another Cisco 3800 series router over an FTC or FTM, the bandwidth required for each circuit is about 2 times the compression rate. For example, adpcm32k requires 76.8k trunk bandwidth, csacelp8k requires 20k. This inefficiency is not present in a circuit between a C3800 and a CDP or CVM on a switch node. There is no workaround.

- CSCdj08918

A PVC configuration and in some cases an SVC configuration can fail to ring both voice ports on the same Rincon simultaneously. The system should ring one port then ring the other then return to ring the first port until they are answered but it will ring one port only and not ring the other until the ringing phone is answered at which time it will then ring the other port correctly. This is dependent on phone type in part and may appear intermittent in different applications. There is no workaround.

- CSCdj09867

Release-note: When a voice port is configure for VAD and coder is set to csacelp, VAD is left inoperative after a reboot. The workaround is to re-establish VAD by entering **no vad** then **vad** for the port. There is no workaround.

- CSCdj11115

Under some configurations, an SNMP poll of the csmStackName MIB object can cause the router to reload. This object exists in the ciscoStackMakerMIB (CISCO-STACKMAKER-MIB.my).

This MIB can essentially be disabled (SNMP is prevented from polling this MIB) via use of SNMP views. This can be changed to: snmp-server view no-stackmib internet included snmp-server view no-stackmib ciscoStackMakerMIB excluded snmp-server community public view no-stackmib ro.

The result is that SNMP polls using the “public” community string can access objects in the entire MIB space (internet) except for those objects in the ciscoStackMakerMIB space.

This workaround will, of course, affect any NMS applications which rely on the ciscoStackMakerMIB objects.

- CSCdj12815

Symptom: Under extremely heavy CPU interrupt states, a router with an FSIP, CT3, or any serial interface might experience the following “output stuck” error message:

```
%RSP-3-RESTART: interface Serial12/0/0:28, output stuck %RSP-3-RESTART: interface Serial12/0/0:6, output stuck %RSP-3-RESTART: interface Serial12/0/0:12, output stuck %RSP-3-RESTART: interface Serial12/0/0:2, output stuck
```

This is a result of a internal timer utility that can incorrectly return a false value under extreme interrupt situations, which causes the transmit buffers backing-store mechanism to falsely declare serial interface “output stuck.”

Conditions: The symptom occurs on Cisco 7000 family routers using the CT3, 4- or 8-port FSIP cards, or any serial interface under Cisco IOS Release 11.1(10)CA, 11.1(11), and 11.2. It is only observed under oversubscribed traffic load conditions.

Workaround: Configure the interface to FIFO queueing using the **no fair-queue** command.

The command **transmit-buffers backing-store** is on by default when an interface is configured for weighted fair-queueing. If the interface command **no fair-queue** is used, which changes the queueing strategy to FIFO, the transmit buffers backing-store is off by default.

- CSCdj17520

During Customer configuration of a 3640 from multiple telnet sessions or from console and a telnet session the following sequence causes a NVRAM corruption:

From one of the sessions: sho conf

From the other session: wr m

These commands occur at the same point in time causing the router to do any of the following: a) Seg V b) PCI Master Abort c) Spurious memory access d) NVRAM corruption e) “trash” displayed to screen of “^@^@^@...”

Interfaces and Bridging

- CSCdj09646

The POS interface specific configuration commands **pos specify-s1s0** and **pos specify-c2** do not work correctly. There is no workaround.

- CSCdj11249

When there is another port adapter (could be another FDDI FDX PA) besides the FDDI FDX port adapter in the same VIP2, the port adapter could hesitate before going into FDX operation. After the port adapter goes into FDX operation, it might fall out of FDX mode for no good reason, and see a large number of claims at the interface. There is no workaround.

- CSCdj11354

On a 7206 running Cisco IOS Release 11.1.10.4 CA1 when ipx route-cache is enabled on an interface clients are unable to connect to novell servers through the router. When ipx route-cache is disabled they are able to connect. There is no workaround.

- CSCdj14850

In 11.1(8)CA images and later, when transparent bridging is configured on the c7200 platform, a system reload can happen under heavy loads. The error message issued by the system will indicate a bus error due to an illegal access to a low address. There is no workaround.

- CSCdj18588

Selecting line (recovered) clocking on the CT3's t1 #23 does not work. There is no known workaround, other than to not do it, i.e. always use internal clocking on t1 #23. Depending on what equipment is at the remote end, this workaround may cause the remote end to slip.

This is fixed in CT3 f/w version 2.2.0. To determine your current CT3 f/w version, use the “show cont t3” exec command:

```
CT3 H/W Version : 5, CT3 ROM Version : 1.2, CT3 F/W Version : 2.2.0 ^^^^^
```

must be 2.2.0 or greater in order to use line clocking on t1 #23.

Other t1s are not affected.

- CSCdj20028

This fix will be checked into cal_p and 11.2(7)P throttle branch. VIP reload due to a NULL pointer (in v0) can now be avoided. There is no workaround.

- CSCdj20356

Multi Channel Interface Processor (MIP), when controller t1 X/X is configured for a pri test on a 7k router instead of the serial X/X:23 interface getting configured, the ether X/X:23 interface gets configured. After this point, any attempt to configure the interface reloads the router. There is no workaround.

Novell IPX, XNS, and Apollo Domain

- CSCdj06068

IPX packets are getting corrupted with MIP and CT3 hardware with fast switching. Work around is to disable ipx fastswitching on these interfaces. There is no workaround.

TCP/IP Host-Mode Services

- CSCdj09782

No more than one DLSw peer comes active in a Cisco 3640 router running Cisco IOS Release 11.1(10). It is possible to configure the second peer, but this one will never be in a CONNECT state.

Workaround: Enter the **no transport input** command on the auxport line.

- CSCdj16381

User Datagram Protocol (UDP) turbo flooding is now supported on the Cisco 3600 series. There is no workaround.

Resolved Caveats—11.2(6)P

This section describes possibly unexpected behavior by Release 11.2(6)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(6)P. For additional caveats applicable to Release 11.2(6)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(6)P.

Basic System Services

- CSCdj19231

A problem has been found in RSP code within Cisco IOS 11.2 P images. The failure condition can occur when BACKING-STORE or fair queuing are enabled. The conditions that could cause one of the above behaviors to occur are expected to be extremely rare.

For those customers running 11.2 P, Cisco highly recommends upgrading all RSP-based systems to one of the Cisco IOS Release 11.2(6)P or later. For those systems that cannot upgrade, this problem can be avoided by disabling both BACKING-STORE and fair queuing. Please see instructions for this at the end of this message.

When packet load on RSP-equipped systems causes datagrams to be forwarded from SRAM to DRAM, a function of BACKING-STORE, 32 bytes of data may be randomly written into DRAM. This could result in several anomalous system behaviors including: - Software-induced system reloads - Dropped datagrams - Other anomalous errors

SOLUTION:

FOR CUSTOMERS WITH Release 11.2 P

Option #1: Cisco highly recommends the installation of 11.2(6)P or later for 11.2(x)P images.

This problem was fixed as bug CSCdi71609 in images 10.3 through 11.2. Unfortunately it was reintroduced as a result of merged code in ONLY 11.2 P.

Option #2: Below are options to work around this bug.

Disable backing store AND fair queuing on each interface with IOS commands

no transmit-buffers backing-store and **no fair-queue**

ALSO disable udp-turbo flooding if the image is 11.0 or later The IOS command to disable UDP turbo flooding is **no ip forward-protocol turbo-flood** which is OFF by default in all releases.

However, it is important to look at the current configuration. An image configured before backing-store defaulted to OFF may have it ON for router interfaces. There is no workaround.

Interfaces and Bridging

- CSCdj01341

When integrated routing and bridging (IRB) is configured on a Cisco 4500 series router in order to route AppleTalk across an Inter-Switch Link (ISL) trunk, the input queue may fill up and stop receiving traffic. There is no workaround.

IP Routing Protocols

- CSCdj04279

On a Cisco 7500 RSP system, access list processing does not work with optimum switching. Packets that should be dropped are forwarded, and packets that should be forwarded are switched via the slower fast switching. The workaround is not to use optimum switching if access lists are defined. There is no workaround.

Wide-Area Networking

- CSCdj07474

In the presence of traffic on the ATM side (LANE configuration), if you reset the ATM module, then wait for the module to come on line and for the first spanning-tree ports (forwarding mode) to show up under the ATM port, then reset the ATM module, it fails to come on line and displays the following error message:

```
CDL-3W-1 (debug-eng) reset 4 Resetting module 4... CDL-3W-1 (debug-eng) Syndiags failed
on Module Number 4 CDL-3W-1 (debug-eng) Wed Apr 2 1997, 16:37:48 Module 4 failed to come
online.
```

At this point, the only workaround is to remove and reinstall the ATM module.

The traffic pattern that caused this had to be “incrementing Destination Address” generated by an Ethernet sniffer. This has been seen with NMP 2.1(705), ATM 3.2(3), and 3.2(2). This will be fixed in ATM 3.2(4). There is no workaround.

Resolved Caveats—11.2(5)P

This section describes possibly unexpected behavior by Release 11.2(5)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(5)P. For additional caveats applicable to Release 11.2(5)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(5)P.

EXEC and Configuration Parser

- CSCdi89723

When you change the encapsulation on an interface from one that supports weighted fair queuing to one that does not and you make the change from the console or auxiliary port, there may be a memory loss of 8 KB each time you change the encapsulation. You can identify this problem by examining the output of the **show memory allocating-process** command, which shows that the number of memory blocks allocated by the EXEC software increases each time you change the encapsulation. If you do not change the encapsulation on an interface often, this problem should not have a significant impact on system performance. There is no workaround.

Resolved Caveats—11.2(4)P

This section describes possibly unexpected behavior by Release 11.2(4)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(4)P. For additional caveats applicable to Release 11.2(4)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(4)P.

Interfaces and Bridging

- CSCdi79832

When pinging over synchronous DDR with HDLC Stacker compression, the router will unexpectedly reset. There is no workaround.

Resolved Caveats—11.2(3)P

This section describes possibly unexpected behavior by Release 11.2(3)P. Unless otherwise noted, these caveats apply to all 11.2 releases up to and including Release 11.2(3)P. For additional caveats applicable to Release 11.2(3)P, see the caveats sections for newer 11.2 releases. The caveats for newer releases precede this section.

All the caveats listed in this section are resolved in Release 11.2(3)P.

IBM Connectivity

- CSCdi73085

A hang of APPN's APPC stack (used to send locates and TDUs) can occur in rare situations when an outbound locate or TDU is in the process of being transmitted on a CP-CP session at the exact time that session is terminated (due to link failure or other reason). The APPC component does not handle this situation properly, and after the condition occurs, APPC and all locates and TDU processing becomes stuck. There is no workaround.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

The most current Cisco documentation is available on the World Wide Web at <http://www.cisco.com>. Translated documentation can be accessed at http://www.cisco.com/public/countries_languages.shtml.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

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

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract. Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

<http://www.cisco.com/tac>

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

<http://www.cisco.com/register/>

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

<http://www.cisco.com/tac/caseopen>

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with release notes for Cisco IOS Release 11.2 P.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0403R)

© 1998–2004, Cisco Systems, Inc.
All rights reserved. Printed in USA