Resolved Caveats—Cisco IOS Release 12.2(13e)

Cisco IOS Release 12.2(13e) is a rebuild release for Cisco IOS Release 12.2(13). The caveats in this section are resolved in Cisco IOS Release 12.2(13e) but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCed28873

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

Miscellaneous

- CSCdx76632

  Symptoms: A Cisco AS5300 that is functioning as a voice gateway may reload because of an incoming bus error exception.

  Conditions: This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(6d).

  Workaround: There is no workaround.

- CSCdx77253

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea32240

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea33065

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea36231

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea46342

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51030

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51076

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea54851

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCeb78836

  Symptoms: Cisco IOS software may cause a Cisco router to reload unexpectedly when the router receives a malformed H.225 setup message.

  Conditions: This symptom is observed on a Cisco 1700 series that runs Cisco IOS Release 12.2(13c). The symptom occurs when the following **debug** privileged EXEC commands are enabled:

  - **debug h225 asn1**
  - **debug h225 events**
  - debug h225 q931

  Workaround: There is no workaround.

- 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 12.2(13c)

Cisco IOS Release 12.2(13c) is a rebuild release for Cisco IOS Release 12.2(13). The caveats in this section are resolved in Cisco IOS Release 12.2(13c) 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.

- CSCdx76632

  Symptoms: A Cisco AS5300 that is functioning as a voice gateway may reload because of an incoming bus error exception.

  Conditions: This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(6d).

  Workaround: There is no workaround.

- CSCdx77253

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCdy61597

  Symptoms: The debug feature for the Q.931 portion of H.225 messages may cause memory corruption.

  Workaround: There is no workaround.

- CSCdz71127

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing

traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

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

This advisory is available at

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

- CSCea02355

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

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

  This advisory is available at

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

- 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.

- CSCea32240

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea33065

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea36231

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea46342

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51030

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51076

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea54851

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCeb78836

  Symptoms: A Cisco router experiences a software forced reload when receiving a malformed H.225 setup message.

  Conditions: These symptoms have been observed on a Cisco 1700 series router running Cisco IOS Release 12.2(13c) when “debug h225 asn1/events/q931” is enabled.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(13b)

Cisco IOS Release 12.2(13b) is a rebuild release for Cisco IOS Release 12.2(13). The caveats in this section are resolved in Cisco IOS Release 12.2(13b) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms: A description of what is observed when the caveat occurs.
- Conditions: The conditions under which the caveat has been known to occur.
- Workaround: Solutions, if available, to counteract the caveat.
- CSCdz49271

  Symptoms: A Cisco 3640 router may not receive Cisco Discovery Protocol (CDP) packets on its Fast Ethernet interface, preventing the router from recognizing its CDP neighbors. Outgoing CDP packets are sent without any difficulties, enabling other devices to recognize the Cisco 3640 router.

  Conditions: This symptom is observed on a Cisco 3640 router that is running Cisco IOS Release 12.2(12.14b).

  Workaround: There is no workaround. If this is an option, downgrade to an earlier release such as Cisco IOS Release 12.2(12b) in which the symptom does not occur.

- CSCea02713

  Symptoms: A router may unexpectedly reload if it is unable to allocate enough memory for Weighted Random Early Detection (WRED). This unexpected reload may also be seen when the interface is already configured for WRED by using modular quality of service (QoS) and when an access group is added to the interface.

  Conditions: This symptom is observed on a router that is running Cisco IOS software that is being configured for WRED on a Frame Relay interface via the modular QoS.

  Workaround: There is no workaround.

- CSCea07020

  Symptoms: A Cisco router that is configured with Frame Relay subinterfaces may leak memory if those subinterfaces are configured with Random Early Detection (RED). If the subinterfaces are configured with RED, other changes to the configuration may cause the router to leak memory as well. For instance, adding an IP access list to a Frame Relay subinterface that is configured with RED will cause the router to leak memory.

  Conditions: This symptom is observed when traffic shaping is configured with RED, which is configured in the subclass in the service policy.

  Workaround: There is no workaround.

- CSCin11611

  Symptoms: Internetwork Packet Exchange (IPX) Enhanced Interior Gateway Routing Protocol (EIGRP) neighbors will not form adjacencies if incremental Service Advertising Protocol (SAP) updates are enabled. IPX EIGRP neighbors will not remain established and IPX routing will not work for interfaces that are affected by this symptom.

  The following message is displayed if the **eigrp log-neighbor-change** router configuration command is configured:

  ```
  %DUAL-5-NBRCHANGE: IPX-EIGRP 1: Neighbor ABC.0001.4266.3381 (Serial0/0)is down: Auth failure
  ```

  Incremental SAP updates are enabled by default on all non-IEEE interfaces (WAN interfaces). Incremental SAP updates are also disabled on all IEEE interfaces (LAN interfaces). Therefore, LAN interfaces are not affected by this symptom unless the interfaces have been configured to perform incremental SAP updates by entering the **ipx sap-incremental** interface configuration command.

  Conditions: This symptom is observed on a Cisco 4224 that is running Cisco IOS Release 12.2(8.05)T.

  Workaround: Configure the **no ipx sap-incremental** interface configuration command on the interfaces that have incremental SAP updates enabled by default or configuration to prevent the symptom from occurring.

Resolved Caveats—Cisco IOS Release 12.2(13a)

Cisco IOS Release 12.2(13a) is a rebuild release for Cisco IOS Release 12.2(13). The caveats in this section are resolved in Cisco IOS Release 12.2(13a) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms: A description of what is observed when the caveat occurs.
- Conditions: The conditions under which the caveat has been known to occur.
- Workaround: Solutions, if available, to counteract the caveat.
- CSCdx39499

  Symptoms: A port adapter may stop receiving packets. When this symptom occurs, the output of the **show interface** EXEC command does not report any input or output drops. When the **show controller** EXEC command is entered on the Versatile Interface Processor (VIP) console of a router, the command output may display incrementing rx_no_buffer and virtual circuit connection (VCC) counts.

  Conditions: These symptoms are observed on the enhanced ATM port adapter (PA-A3) of a Cisco 7500 series.

  Workaround: Bounce the port adapter interface by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCdy30984

  Symptoms: Transmit and receive statistics counters may show inaccurate numbers for some interfaces.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround when compression is disabled on the interface. If compression is enabled on the interface, the **show compress** EXEC command can be entered to obtain transmit and receive statistics.

- CSCdy41378

  Symptoms: IP Security (IPSec) may fail to encrypt traffic when the hardware crypto accelerator is used and when Fast switching or Cisco Express Forwarding (CEF) switching is enabled. The hardware crypto accelerator may return the following error message:

  ```
  %VPN_HW-1-PACKET_ERROR: slot: 0 Packet Encryption/Decryption error, Invalid Packet
  ```

  Conditions: The symptom is observed with almost all types of IPSec configurations. The symptom is prevalent when there is Layer 2 (L2) padding in the packet.

  Workaround: There is no workaround.

- CSCdy54385

  Symptoms: After a second switchover occurs, a Cisco 7200 series or Cisco 7500 series router that is functioning as a backup router becomes active and the primary router goes into standby mode, but the Cisco 7200 series or Cisco 7500 series router may fail to handle connections that are directed at its virtual Hot Standby Router Protocol (HSRP) address and may not respond to pings that are directed at its HSRP address at the client side, server side, or both.

  Conditions: These symptoms are observed when you use a Cisco Catalyst 6000 series switch as the primary router and a Cisco 7200 series or Cisco 7500 series router as a backup router that is configured with a 2-port Fast Ethernet/Inter-Switch Link (ISL) port adapter (PA-2FEISL) that has at least one Fast Ethernet interface configured for HSRP, and when a second switchover occurs. The symptom occurs only with Fast Ethernet interfaces of a specific third-party vendor.

The symptoms occur because the Fast Ethernet interface that is configured for HSRP is not switched to promiscuous mode when the HSRP group becomes active for the second time, preventing packets that are addressed to the HSRP virtual MAC address from being received by the interface. The output of the **show controllers fastethernet** EXEC command displays whether the promiscuous mode is enabled or disabled.

Reboot the Cisco 7200 series or Cisco 7500 series router to restore the router to proper backup operation.

Workaround: Enable the **standby use-bia** interface configuration command on the HSRP interface.

- CSCdy59613

  Symptoms: A software-forced reload may occur on a router.

  Conditions: This symptom is observed when a dialer trigger call is made on platforms that support ISDN and dialer.

  Workaround: There is no workaround.

- CSCdy63773

  Symptoms: Call setup may not work as expected.

  Conditions: This symptom is observed on a vendor-specific private automatic branch exchange (PABX) after a connected Cisco router is upgraded to Cisco IOS Release 12.2(12).

  Workaround: There is no workaround.

- CSCdy80595

  Symptoms: The Versatile Interface Processor (VIP) disabling feature is not working as expected. After the VIP reloads, it remains disabled even after an online insertion and removal (OIR) is performed on the VIP.

  Conditions: This symptom is observed when the OIR Remove Failing Slot (ORFS) feature is configured. The VIP is disabled after it reloads a certain number of times.

  Workaround: Enter the **show rsp orfs-info** EXEC command to display the configured parameters for the service ORFS. After learning about the configured parameters for the service ORFS, you may enter the **no service oir-remove-failing-slot** *slot number* **reload-limit** *reload-limit* global configuration command to bring up a particular line card, or you may enter the **no service oir-remove-failing-slot** global configuration command to bring up all disabled cards.

- CSCdz17156

  Symptoms: This caveat relates to two issues that are observed with two-stage calls.

  a. The second number is disconnected by a router if a dial peer is not found (with an unallocated number cause code). The PBX on the originating leg of the call then sends a disconnect with progress indicator (PI) signal. After the disconnect with PI signal is sent, the router does not send an ISDN release message as expected. Instead, the router waits 30 seconds for the ISDN T306 timer to expire.

  b. The originator disconnects after the second-stage call receives the alerting message. The call is not released for 30 seconds while the router waits 30 seconds for the ISDN T306 timer to expire.

  Conditions: These symptoms are observed when an ISDN disconnect with PI signal is received from the first leg of a call. Both of these issues are observed with two-stage calls.

  Workaround: There is no workaround, but the call will be released after 30 seconds.

- CSCdz22927

  Symptoms: PPP Link Quality Monitoring (PPP-LQM) may fail to maintain link quality.

Conditions: This symptom is observed when PPP-LQM is enabled with hardware compression (PA-COMP) on a Cisco 7200 series.

Workaround: Disable hardware compression and use software compression when PPP-LQM is required.

- CSCdz35882

  Symptoms: More than 128 interfaces may fail to come up on an enhanced 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+). The 129th channel will fail to come up, and the following message may be displayed:

  ```
  %MCX-1-STARTFAIL: Serial1/0:27 channel not enabled
  ```

  Conditions: This symptom is observed when 128 interfaces are configured on a PA-MC-8TE1+ port adapter of a Cisco router that is running Cisco IOS Release 12.2(12a).

  Workaround: There is no workaround.

- CSCdz37574

  Symptoms: If a transient failure occurs in a Frame Relay network and causes three or more Voice over Frame Relay (VoFR) permanent virtual circuit (PVC) keepalive messages to be lost, the PVC will stop sending keepalive messages and will not start sending the keepalive messages again until the next outgoing call is placed. This behavior will occur if Frame Relay Local Management Interface (LMI) messages are not disturbed by the transient failure.

  Conditions: When the transient failure occurs, some PVC keepalives may be lost (but no LMI messages are lost) and PVC keepalives will be turned off. PVC keepalives should not be turned off when the transient failure occurs.

  The disabling of the PVC keepalives is not dependent on whether LMI messages are lost. If the transient failure persists for a sufficient period of time, LMI messages will be lost and Layer 2 will be marked down. When Layer 2 is marked down, PVC keepalives will also be turned off. The PVC keepalives will be restarted after Layer 2 recovery occurs.

  Workaround: There is no workaround.

- CSCdz40567

  Symptoms: Counter overflow errors may be observed with the IP protocol on a serial interface.

  Conditions: This symptom is observed on the serial interface of a Cisco 7500 series.

  Workaround: There is no workaround.

- CSCdz51138

  Symptoms: An incorrect value is displayed for the ifOperStatus object for High-Speed Serial Interfaces (HSSIs) that are running PPP or propPointToPointSerial encapsulation. A value of “6” (not present) is returned.

  Conditions: This symptom is observed when a Simple Network Management Protocol (SNMP) query is performed on the ifOperStatus object or the propPointToPointSerial encapsulation.

  Workaround: There is no workaround.

- CSCdz52774

  Symptoms: A router may reload because of illegal access to a low address. This symptom is observed if a particular race condition occurs when a delete context request is received by Gateway General Packet Radio Service (GPRS) Support Node (GGSN) before a create response is sent back by GGSN for a packet data protocol (PDP) context.

Conditions: This symptom is observed on a Cisco 7200 series that is running a GGSN image of Cisco IOS Release 12.2(12). This symptom is observed under a rare condition after RADIUS authentication and authorization have successfully occurred. Before a create response is sent, the process is suspended and a PDP context is deleted in a different process flow.

Workaround: There is no workaround.

- CSCdz60229

  Cisco devices which run IOS and contain support for the Secure Shell (SSH) server are vulnerable to a Denial of Service (DoS) if the SSH server is enabled on the device. A malformed SSH packet directed at the affected device can cause a reload of the device. No authentication is necessary for the packet to be received by the affected device. The SSH server in Cisco IOS is disabled by default.

  Cisco will be making free software available to correct the problem as soon as possible.

  The malformed packets can be generated using the SSHredder test suite from Rapid7, Inc. Workarounds are available. The Cisco PSIRT is not aware of any malicious exploitation of this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml

- CSCdz61466

  Symptoms: A Virtual Private Network (VPN) may stop working under rare traffic conditions.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(13) and that is using one of the following VPN cards:

  - Basic performance VPN encryption asynchronous interface module (AIM-VPN/BP)
  - Enhanced performance VPN encryption AIM (AIM-VPN/EP)
  - High performance VPN encryption AIM (AIM-VPN/HP)
  - Encryption network module (NM) (NM-VPN/MP)

  Workaround: Disable hardware encryption.

- CSCdz65899

  Symptoms: The following CPU hog message may be displayed on a router after a multilink interface is shut down:

  ```
  %SYS-3-CPUHOG: Task ran for 2480 msec (3/2), process = Multilink
  ```

  Conditions: This symptom is observed when a state transition occurs on a multilink interface such as when the interface is coming up or going down.

  Workaround: There is no workaround for the CPU hog condition.

  If any application or routing protocol is affected by the CPU hog condition and is consequently timing out, you can increase the duration of the application or routing protocol timers.

- CSCdz71171

  Symptoms: A router may report a loss of signal indication on all 28 T1 lines. When this symptom occurs, MIB updates that are being sent from a Route Switch Processor (RSP) to a Versatile Interface Processor (VIP) may stop.

  Conditions: This symptom is observed on a Cisco 7500 series that has channelized T3 (CT3) port adapters.

  Workaround: There is no workaround.

- CSCdz75118

  Symptoms: The interface input rate and output rate counters that are reported in the output of the **show interface** EXEC command do not decrease to zero after the interface is administratively shut down. The counters show the last input and output rates that were observed while the interface was up. The following output may be observed when the **show interface serial 2/1/0** EXEC command is entered on the affected interface:

  ```
  Router> show interface serial 2/1/0
  Serial2/1/0 is administratively down, line protocol is down
  30 second input rate 466000 bits/sec, 560 packets/sec
  30 second output rate 466000 bits/sec, 560 packets/sec
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.2(13) and that has an Ethernet, Fast Ethernet, Gigabit Ethernet, ATM, inverse multiplexing over ATM (IMA), or serial interface. This symptom does not affect channelized serial interfaces.

  Workaround: There is no workaround.

- CSCdz85565

  Symptoms: A Cisco 7200 series router may cause IP header compression regression tests to fail when fast-switched packets are being counted as process-switched packets.

  Conditions: This symptom is observed on M4T interfaces only.

  Workaround: There is no workaround.

- CSCin25008

  Symptoms: A Cisco 7500 series may reload.

  Conditions: This symptom is observed after an online insertion and removal (OIR) is performed on the Versatile Interface Processor (VIP) of a Cisco 7500 series. This symptom is observed if the 8-port T1 inverse multiplexing over ATM (IMA) port adapter (PA-A3-8T1) or the 8-port E1 IMA port adapter (PA-A3-8E1) is installed on the VIP.

  Workaround: There is no workaround.

- CSCin26892

  Symptoms: Input counters and rate counters may display a zero value.

  Conditions: This symptom is observed on a Cisco 7500 series that has an 8-port enhanced multichannel T1/E1 port adapter that has a channel service unit/data service unit (CSU/DSU) (PA-MC-8TE1+) or a PA-CE3 interface.

  Workaround: You may display Input counters by entering the **show interface serial stats** EXEC command. There is no alternate way to display the input rate counters.

Resolved Caveats—Cisco IOS Release 12.2(13)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(13). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(13). This section describes severity 1 and 2 caveats and select severity 3 caveats.

The following information is provided for each caveat:

- **Symptoms**—A description of what is observed when the caveat occurs.
- **Conditions**—The conditions under which the caveat has been known to occur.
- **Workaround**—Solutions, if available, to counteract the caveat.

Basic System Services

- CSCdu88223

  Symptoms A serial interface may show an interface as down/down even when all signals (request to send [RTS], clear to send [CTS], data terminal ready [DTR], data carrier detect [DCD]) are present.

  Conditions This symptom is observed on the serial interface of a Cisco router that is running Cisco IOS Release 12.0(15).

  Workaround Reload the microcode.

- CSCdv18909

  Symptoms A router may be restarted by a bus error. The following is a stack trace of the failure:

  ```
  FP: 0x6167F848, RA: 0x603F49C8 FP: 0x6167F878, RA: 0x603F24B4 FP: 0x6167F898,
  RA: 0x60376528 FP: 0x6167F8C0, RA: 0x60388C98 FP: 0x6167F8F0, RA: 0x60388CE8
  FP: 0x6167F908, RA: 0x60337D08 FP: 0x6167FA40, RA: 0x603F24B4 FP: 0x6167FA60,
  RA: 0x60A55078
  ```

  Conditions This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.1(9).

  Workaround There is no workaround.

- CSCdv42950

  Symptoms The following message is displayed when the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command is entered on an interface on a 4-port serial port adapter (PA-4T+) or an 8-port serial port adapter (PA-8T):

  ```
  %VIP-3-BADMALUCMD: VIP2 slot0: Unsupported MALU command 35, arg=0x0, pascb=0x60B61100
  ```

  Conditions This symptom is observed on a Cisco Route Switch Processor that is running Cisco IOS Release 12.2(10a).

  Workaround There is no workaround.

- CSCdw71371

  Symptoms When an autoinstallation is performed on a router, the router successfully downloads the configuration but pauses to display the “Do you want to enter the initial configuration dialog?” prompt. The router boots up completely only after the “n” character is issued at the prompt.

  Conditions This symptom is observed on a Cisco 2621 router that is running Cisco IOS Release 12.2(6). This symptom occurs if the downloaded configuration contains an encapsulation type that is different from the encapsulation type that is configured on the peer router to which the Cisco 2621 is connected.

  Workaround Ensure that the encapsulation type that is on the downloaded configuration is the same as the encapsulation type that is on the peer router.

- CSCdx52334

  Symptoms A server may report the absence of an access list after the server has rebooted.

  Conditions This symptom is observed on a network access server (NAS) that is running Cisco IOS Release 12.2(02)XB05.

Workaround There is no workaround.

- CSCdx68230

  Symptoms A CPU hog condition may be observed on a router, and the router may reload.

  Conditions These symptoms are observed when the **snmp-server community** global configuration command is executed on a Cisco router that is running Cisco IOS Release 12.1 and that has several thousand logical entities configured.

  Workaround There is no workaround.

- CSCdx82485

  Symptoms Under rare circumstances, a router that is configured with Protocol-Independent Multicast (PIM) may pause indefinitely.

  Conditions This symptom is observed when an interface that has PIM enabled is shut down. This symptom may also occur when other configuration operations are performed on a PIM-enabled interface. This symptom affects only port adapters such as the 8-port 10BASE-T Ethernet port adapter (PA-8E) and the 8-port 10BASE-T Ethernet port adapter (PA-4E) that are using a particular third-party vendor chip.

  Workaround Use a different Ethernet card, or avoid using PIM.

- CSCdx85827

  Symptoms The following traceback messages are displayed when a load test is performed:

  ```
  %AAAA-3-BADSTR: Bad accounting data: too many attributes
  -Traceback= 60315CB8 603196CC 6022CABC 601C62A0 601C6DB8 601F39D8 601F5BA0 601F723C
  %AAAA-3-BADSTR: Bad accounting data: too many attributes
  -Traceback= 60315CB8 603196CC 6022CABC 601DA818 601DA9C4 601F5374 601F7294
  ```

  Conditions This symptom is observed on a Cisco AS5400 universal access server that is tested with 548 calls at 4 to 6 calls per second (cps).

  Workaround There is no workaround.

- CSCdy02831

  Symptoms A Multilayer Switch Feature Card 2 (MSFC2) may reload when the **no ip routing** global configuration command is entered.

  Conditions This symptom is observed on a Catalyst 6000 MSFC2 that is running Cisco IOS Release 12.1(12)E.

  Workaround Do not disable IP routing on the MSFC2.

- CSCdy04066

  Symptoms The “no MIB objects contained under subtree” message is displayed when a Simple Network Management Protocol (SNMP) walk is performed on RFC1406-MIB DS1 objects.

  Conditions This symptom is observed on a Cisco MC3810 router that is running Cisco IOS Release 12.2(6f).

  Workaround There is no workaround.

- CSCdy04472

  Symptoms Polling for numbered ATM subinterfaces and unnumbered Frame Relay interfaces does not return any data. When the ifInNUcastPkts, ifOutNUcastPkts, and ifOutQLen variables are among the first of multiple objects that are bundled together in an **snmpget** command, some or all of these variables return the message “no such variable.”

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.0(19)S2.

Workaround Retrieve the variables individually or via an **snmpwalk** command.

- CSCdy14424

  Symptoms A repeatedly reloading Versatile Interface Processor (VIP) may cause a network outage.

  Conditions This symptom is observed when there is a faulty VIP or faulty hardware in the chassis.

  Workaround There is no workaround.

- CSCdy18495

  Symptoms After a gateway controller goes down or becomes disconnected from a network, the gateway still shows that the permanent virtual circuits (PVCs) are in the up state. Traffic cannot be sent if the PVCs remain in the up state.

  Conditions This symptom is observed on a Cisco MC3810 that is running Cisco IOS Release 12.2(2)XB5.

  Workaround Enable the **oam-pvc manage** interface-ATM-VC configuration command.

- CSCdy20322

  Symptoms A router that is configured for TACACS+ may run out of memory because of a buffer leak in the middle buffer pool that is caused by TACACS+ packets. The occurrence of this symptom can be verified by entering the **show buffers** EXEC command or the **show tcp brief all** EXEC command on the router.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.0(15).

  Workaround Reload or power-cycle the router to free the buffers and memory.

- CSCdy29329

  Symptoms The cache error recover function (CERF) is disabled after a Cisco 7200 series router is reloaded. This symptom is observed after CERF is enabled, written into the startup configuration, and the router is reloaded.

  The output of the **show memory cache error-recovery** EXEC command may indicate that the commands are disabled after the router is reloaded:

  ```
  no memory cache error-recovery L3 data
  no memory cache error-recovery options nvram-report
  no memory cache error-recovery options parity-check
  memory cache error-recovery options window 0
  memory cache error-recovery options max-recoveries 0
  ```

  Conditions This symptom is observed on a Cisco 7200 series router that is using a Network Processing Engine (NPE-300) that has 32 MB of memory in the dual in-line memory module (DIMM2).

  Workaround Install 64 MB of memory in the DIMM2.

- CSCdy52901

  Symptoms A Cisco 7206VXR router may reload with a bus error after the following error message is generated:

  ```
  %AAAA-3-LOSTTIMER: Lost periodic accounting timer for user.
  ```

  Conditions This symptom is observed on a Cisco 7206VXR router that is running Cisco IOS Release 12.2(10a) and that has periodic accounting enabled.

  Workaround Disable periodic accounting.

- CSCdy62338

  Symptoms The **show bootflash: chips** EXEC command may cause subsequent commands such as the **show bootflash all** EXEC command to fail.

  Conditions This symptom is observed on a Cisco router that has a Route Switch Processor (RSP8) and that is running Cisco IOS Release 12.2(6d) or Release 12.2(6f). This symptom occurred only because the bootflash module was flawed.

  Workaround Enter the **show version** EXEC command to restore the router to normal operating condition.

- CSCdy65626

  Symptoms When vendor-specific Challenge Handshake Authentication Protocol (CHAP) authentication is used, a router may reload if an incorrect key is configured and if the **debug tacacs** EXEC command is enabled.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(12.06) or Release 12.2(12.05)S.

  Workaround Ensure that the key is correct, or disable the **debug tacacs** EXEC command.

- CSCdy80552

  Symptoms A memory leak in the ISDN process may cause a Cisco AS5xxx voice gateway that is operating under stress conditions to reload.

  Conditions This symptom is observed when more than one host that uses the Simple Network Management Protocol version 1 (SNMPv1) security model is configured on the router by entering the **snmp-server host** *host-addr* global configuration command such as in the following configuration:

  ```
  snmp-server host 10.30.50.41
  snmp-server host 10.30.50.40
  ```

  Workaround Remove the multiple instances of configured SNMPv1 hosts. Only one host should be specified in the running configuration by entering the **snmp-server host** *host-addr* global configuration command.

- CSCin10634

  Symptoms A Cisco 7500 series router may reload because of a software condition after an online insertion and removal (OIR) of a Versatile Interface Processor (VIP) that is configured with an ATM OC-3c/STM-1 port adapter (PA-A3-OC3) and after the following error message has been generated:

  ```
  %SYS-6-STACKLOW: Stack for process OIR Handler running low, 12/3000
  ```

  Conditions This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2(7) and occurs with a VIP2-50, VIP4, and VIP6. The symptom is related to the PA-A3-OC3 and occurs only during an OIR.

  Workaround Do not perform an OIR on any VIP that is configured with a PA-A3-OC3.

- CSCin19616

  Symptoms A router may reload if the Service Assurance Agent (SAA) FTP probe is configured and deleted after it is started through the Simple Network Management Protocol (SNMP) using an FTP server name that is not recognized by the router.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(1).

Workaround Perform either one of the following steps for the workaround:

a. Specify an IP address instead of a server name:

```
rttMonEchoAdminURL.2 -D ftp://rtr:rtr@172.16.0.0/trip
```

b. Configure the **ip host** *name address1* global configuration command (in the example below, "SAA-NMS" is the *host* argument and "172.16.0.0" is the *address1* argument) before configuring the FTP operation on the router:

```
ip host saa-nms 172.16.0.0
rttMonEchoAdminURL.2 -D ftp://rtr:rtr@saa-nms/trip
```

- CSCuk36939

  Symptoms Cisco IOS software fails to set up the Gigabit Ethernet Interface Processor (GEIP) MIBs correctly on a Cisco 7500 series router.

  Conditions This symptom is observed when the hierarchy on the GEIP is incorrect; the port adapter and interface are shown at the same level as the GEIP. The GEIP should be at the top of the hierarchy, followed by the port adapter, followed by the interface.

  Workaround There is no workaround.

IBM Connectivity

- CSCdv53806

  Symptoms A router may reload with a bus error.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.1(9) with data-link switching (DLSw).

  Workaround There is no workaround.

- CSCdx93532

  Symptoms A router may reload when the **dlsw transparent redundancy-enable** interface configuration command is removed from and reapplied to the Ethernet interface.

  Conditions This symptom is observed when the **dlsw transparent redundancy-enable** interface configuration command is removed from and reapplied to the Ethernet interface on a Cisco router that is using data-link switching (DLSw) Ethernet redundancy while there may be multiple circuits between the same pair of MAC addresses that are on different service access points (SAPs).

  Workaround Use DLSw with transparent bridging instead of using the DLSw Ethernet redundancy feature.

- CSCdx94359

  Symptoms Cisco Express Forwarding (CEF) does not route packets to a Channel Interface Processor (CIP) Common Link Access for Workstations (CLAW) backup host.

  Conditions This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.1(15). The CIP in the setup is configured using CLAW backup.

  This symptom does not occur when there is an active CLAW connection to the primary host; rather, occurs when there is an active CLAW connection to the backup host. IP connectivity to the host IP address fails when an attempt is made to traverse an ingress interface that has CEF enabled. Full IP connectivity is restored if CEF is disabled on the ingress interface. The host IP address can be pinged from the CIP router but not from another device that is attached to an interface on the CIP router that has CEF enabled.

Workaround Disable CEF by entering the **no ip route-cache cef** global configuration command on the ingress interface.

- CSCdy00218

  Symptoms A Synchronous Data Link Control (SDLC) session enters the down state (no response and no polling) after an I-Frame is sent. SDLC sessions pause indefinitely if the **simultaneous** keyword is used in the interface configuration for the serial SDLC interface. No polling is observed when this symptom occurs.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(10).

  Workaround Do not use the **simultaneous** keyword in the configuration of the SDLC serial interface.

- CSCdy09312

  Symptoms Spurious memory access may be observed on a router when the **dlsw bgroup-list** global configuration command is removed from the configuration.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(5.08).

  Workaround Modify the configuration after the router is brought offline.

- CSCdy17815

  Symptoms A router may reload unexpectedly and display the following message:

  ```
  System was restarted by bus error at PC 0x60F16C2C, address 0xD0D0D1D at 09:33:36 mest
  4500 Software (C4500-A3JS-M), Version 12.2(8.1), MAINTENANCE INTERIM SOFTWARE
  Compiled (current version) Image text-base: 0x60008948, data-base: 0x61116000
  ```

  Conditions This symptom is observed on a Cisco 4500 series router that is running Cisco IOS Release 12.2(8.1) and that has data-link switching (DLSw) services and a Systems Network Architecture Switching Services (SNASw) switch configured.

  Workaround There is no workaround.

- CSCdy17832

  Symptoms A router may reload with a bus error at the CLSDluCheck process and display the following message:

  ```
  CLS: Assertion failed: file "../cls/cls_entitymanager.c", line 447
  ```

  Conditions This symptom is observed on a router that is running Cisco IOS Release 12.2(5) and that has data-link switching (DLSw) services and a Systems Network Architecture Switching Services (SNASw) switch configured.

  Workaround There is no workaround.

- CSCdy47735

  Symptoms A Cisco 3600 series router and a Cisco MC3810 may reload because of a software condition.

  Conditions This symptom is observed on a Cisco 3600 series router and a Cisco MC3810 that are both running Cisco IOS Release 12.2(8)T5 or Release 12.2(11)T when a peer goes down, the serial tunnel (STUN) to the peer goes down, and after a while the Cisco 3600 series router and the Cisco MC3810 attempt to connect again to the peer.

  Workaround There is no workaround.

Interfaces and Bridging

- CSCdw41164

  Symptoms A Versatile Interface Processor (VIP) may reload because of an error at the ct3sw_check_tx process.

  Conditions This symptom is observed on a Cisco 7000 series VIP that is running Cisco IOS Release 12.0(16)S4.

  Workaround There is no workaround.

- CSCdx00274

  Symptoms A single-port Fast Ethernet 100BASE-TX port adapter (PA-FE-TX) on a Cisco 7206VXR router that has a Network Processing Engine (NPE-300) may stop receiving burst traffic packets.

  Conditions This symptom is observed on a PA-FE-TX on a Cisco 7206VXR that has a Network Processing Engine (NPE-300).

  Workaround This symptom can be cleared by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the PA-FE-TX interface.

- CSCdx53873

  Symptoms Multiprotocol Label Switching (MPLS) packets that are greater than 1498 bytes may not be received on a router.

  Conditions This symptom is observed on a Cisco 7500 router that is running Cisco IOS Release 12.2(10a) and that is using dot1q encapsulation.

  Workaround There is no workaround.

- CSCdx74796

  Symptoms Traceback messages that are related to memory allocation are displayed when a channelized T1 (CT1) or a channelized E1(CE1) port adapter is shut down.

  Conditions This symptom is observed on a Cisco 7200 router that is connected to a Cisco 2600 router through an ISDN switch.

  Workaround There is no workaround.

- CSCdx84379

  Symptoms Packet drops may be observed.

  Conditions This symptom is observed on a channelized T1 (CT1) interface between a provider edge router (PE) and a customer edge (CE) router.

  Workaround There is no workaround.

- CSCdx84574

  Symptoms A Versatile Interface Processor (VIP) may reload and restart after a Fast Ethernet port adapter (PA-FE) is installed.

  Conditions This symptom is observed on a VIP that is installed in a Cisco 7500 series router.

  Workaround There is no workaround.

- CSCdy03204

  Symptoms An Ethernet driver on an Ethernet interface may receive and forward packets that are not destined for itself.

  Conditions This symptom is observed on an Ethernet interface that has the promiscuous mode enabled in a network that has multiple Hot Standby Router Protocol (HSRP) groups. This symptom is also observed when no transparent bridging is occurring.

  Workaround There is no workaround.

- CSCdy09469

  Symptoms End stations may not be able to recognize the data link control (DLC) header because the Cisco IOS software sets an incorrect DLC header on 802.1Q packets by shifting two bytes to the right.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround Use a nonnative VLAN identification (ID).

- CSCdy09509

  Symptoms A buffer leak may be observed in the small buffers on a router.

  Conditions This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(10a) and that is using distributed Link Fragmentation and Interleaving (dLFI).

  Workaround There is no workaround.

- CSCdy23165

  Symptoms Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) traffic may not pass through a port adapter.

  Conditions This symptom is observed on a Cisco 7500 router that has either a 2-port Fast Ethernet 100BASETX (PA-2FE-TX) or a 2-port Fast Ethernet 100BASE-FX (PA-2FE-FX) port adapter. This symptom is observed when OSPF and EIGRP are configured on either the PA-2FE-TX or the PA-2FE-FX port adapter. The port adapter interface does not form the adjacency because multicast entries are not added to the hardware address filter.

  Workaround Enter the **ip pim** interface configuration command on the port adapter interface to clear the condition.

- CSCdy24803

  Symptoms The output of the **show interface atm x/y** EXEC command shows that the inbytes counter decreases when the inpackets counter increases.

  Conditions This symptom is observed on an Enhanced ATM port adapter (PA-A3) that is installed on a Cisco 7200 router.

  Workaround There is no workaround.

- CSCdy32609

  Symptoms When the size of the maximum transmission unit (MTU) on an ATM subinterface is modified, the MTU of virtual circuits (VCs) that are configured under that subinterface are set to 0, and the subinterface cannot be pinged.

  Conditions This symptom is observed on a Cisco 7500 router.

  Workaround There is no workaround.

- CSCdy38335

  Symptoms A router that is configured with a 2-port Fast Ethernet 100BASE-FX port adapter (PA-2FE-TX) may reload when the packet cleanup is not performed properly in the interrupt path of the port adapter.

  Conditions This symptom is observed on a Cisco 7200 series router and a Cisco 7500 series router.

  Workaround There is no workaround.

- CSCdy43105

  Symptoms The 2-port Fast Ethernet 100BASE-TX port adapter (PA-2FE-TX) of a Cisco 7500 series router may not receive Inter-Switch Link (ISL) multicast traffic when ISL is configured on the PA-2FE-TX port adapter. ISL traffic is not received on the PA-2FE-TX port adapter because multicast range entries for ISL are not populated on the port adapter.

  Conditions This symptom is observed when ISL is configured on the PA-2FE-TX of a Cisco 7500 series router that is running Cisco IOS Release 12.2(12.02)T1.

  Workaround There is no workaround.

- CSCdy47536

  Symptoms A Route Switch Processor (RSP) on a router may reload when a subinterface of a 1-port Fast Ethernet 100BASE-TX port adapter (PA-FE-TX) that is configured with dot1q encapsulation is removed.

  Conditions This symptom is observed on the RSP of a Cisco router that is running Cisco IOS Release 12.2(12.5). The RSP card has a PA-FE-TX port adapter with a subinterface that is configured with dot1q encapsulation.

  Workaround Shut down and remove the subinterface that is configured with dot1q encapsulation.

- CSCdy51658

  Symptoms Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) updates are not received on a single-port Fast Ethernet 100BASE-TX port adapter (PA-FE-TX) of a Cisco 7200 series. The PA-FE-TX port adapter does not receive the OSPF, EIGRP, and RIP updates on the Cisco 7200 series because multicast entries are not added in the hardware address filter.

  Conditions This symptom is observed on a PA-FE-TX port adapter of a Cisco 7200 series.

  Workaround Reset the affected interface by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command. When the interface comes back up, it will function normally and receive the routing updates.

- CSCdy71361

  Symptoms Bridged traffic may not be forwarded on a serial interface that is in the down (looped) state if the Spanning-Tree Protocol (STP) is disabled on the interface.

  Conditions This symptom is observed on the serial interface of a Cisco router that is running Cisco IOS Release 12.2(7a).

  Workaround Avoid enabling the following commands together:

  ```
  down-when-looped
  bridge-group 1 spanning-disabled
  ```

- CSCdy80866

  Symptoms When you configure more than 64 Inter-Switch Link (ISL) VLANs, a Versatile Interface Processor (VIP) may reload.

  Conditions This symptom is observed on a Cisco 7500 series router.

  Workaround Use only dot1q encapsulation.

- CSCdy89508

  Symptoms A channelized T1 (CT1) port adapter on a Cisco 7500 series router may not come up.

  Conditions This symptom is observed on a Cisco 7500 series that is running an rsp-jsv-mz image of Cisco IOS Release 12.2(12.10)T1.

  Workaround Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the Cisco 7500 series.

- CSCdy89663

  Symptoms A Cisco 12000 series router may reload when an interface flaps.

  Conditions This symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(21)S during multicast traffic.

  Workaround There is no workaround.

- CSCdz05995

  Symptoms The output of the **show compress** EXEC command may be incorrect.

  Conditions This symptom is observed when PPP compression, High-Level Data Link Control (HDLC) compression, or Frame Relay compression is configured on a router.

  Workaround There is no workaround.

- CSCin11537

  Symptoms An ATM interface may not come up after the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command is entered.

  Conditions This symptom is observed on a Catalyst 5000 Route Switch Module (RSM) that is running Cisco IOS Release 12.2(10).

  Workaround There is no workaround.

- CSCin16267

  Symptoms The packets on an 802.1q subinterface of an AMDP2 Ethernet interface on nondistributed platforms such as a Cisco 7200 series router are not switched by Cisco Express Forwarding (CEF). The packets are not switched by either CEF or distributed Cisco Express Forwarding (dCEF) on a Cisco 7500 series router.

  Conditions This symptom is observed on the Cisco 7200 series and Cisco 7500 series routers.

  Workaround There is no workaround.

- CSCin16706

  Symptoms Open Shortest Path First (OSPF) multicast packets are not received on a 1-port Fast Ethernet 100BASE-TX port adapter (PA-FE-TX).

  Conditions This symptom is observed on a PA-FE-TX port adapter on a Cisco 7500 router that is configured with OSPF. The PA-FE-TX does not receive OSPF multicast traffic because MAC multicast entries are not added to the MAC table.

  Workaround There is no workaround.

IP Routing Protocols

- CSCdx32611

  Symptoms After you detach an interface from a Virtual Private Network (VPN) routing/forwarding (VRF) instance using the **no ip vrf forwarding** *vrf-name* command, the adjacency information that is associated with the removed interface still shows up in the VRF table.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdx83729

  Symptoms A summarized entry may remain in the Enhanced Interior Gateway Routing Protocol (EIGRP) topology table after manual summarization is disabled.

  Conditions This symptom is observed when manual summarization is enabled and subsequently disabled on a network that is also being redistributed into EIGRP.

  Workaround Restart the EIGRP process.

- CSCdx86289

  Symptoms A memory leak may occur on a router. Background processes, route flapping, and the presence of a large number of routes in the global routing table may expedite the memory leak.

  Conditions This symptom is observed on a Cisco router.

  Workaround Upgrade to the latest Cisco IOS release.

- CSCdx92116

  Symptoms Connectivity issues may be observed between a primary link and a backup link when the connection is switched back to the primary link.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(7a) and that has Port Address Translation (PAT) running over a primary link and a backup link. The connectivity issues occur because the inside global PAT address is still referred to as the one from the backup link when the connection is switched from the backup link to the primary link.

  Workaround Clear up the Network Address Translation (NAT) by entering the **ip nat clear translation *** global configuration command after the connection switches back to the primary link.

  Alternate Workaround Configure a short translation timeout value.

- CSCdx96243

  Symptoms A router that is installed with wildcard filter Resource Reservation Protocol (RSVP) flows does not show traffic statistics for the flow in the output of the **show ip rsvp installed detail** EXEC command.

  Conditions This symptom is observed on a Cisco 2600 router that is running Cisco IOS Release 12.2(10).

  Workaround Configure the receiver to issue fixed filter reservations or shared-explicit reservations.

- CSCdy04712

  Symptoms A router that is configured with the neighbor *address* or the **neighbor ibgp peer-group** *name* **nlri unicast multicast** Border Gateway Protocol (BGP) commands does not automatically translate the **no auto-summary** command into the multicast address family.

  Conditions The symptom is observed on a Cisco router when more than one address family is used under BGP.

  Workaround Manually add the **no auto-summary** command into the multicast address family.

- CSCdy05135

  Symptoms If Network Address Translation (NAT) overload is configured, translation may not function properly. A packet may be translated twice, and the inside global address may be considered as the inside local address.

  Conditions This symptom is observed on a Multilayer Switch Feature Card (MSFC2) that is running Cisco IOS Release 12.1(2)E or Release 12.1(8b)E9.

  Workaround Configure an access list for the NAT dynamic mappings, that would permit inside hosts only.

- CSCdy13646

  Symptoms A Cisco 12416 router may reload because of a watchdog timeout in the Border Gateway Protocol (BGP) I/O process.

  Conditions This symptom is observed when a Cisco 12416 router that is configured with 575 BGP peers and three 1-port OC-12 ATM line cards, each of which is configured with 500 ATM permanent virtual connection (PVC) subinterfaces, is booted with Cisco IOS Release 12.0(22)S.

  Workaround There is no workaround.

- CSCdy23229

  Symptoms A Cisco 2611 may reload after a new configuration is downloaded using TFTP. There were no major changes to the configuration after the configuration file was downloaded.

  Conditions This symptom is observed on a Cisco 2611 that is running Cisco IOS Release 12.1(5)T9.

  Workaround There is no workaround.

- CSCdy32096

  Symptoms Delays, loss of synchronization, and packet loss may be observed with voice or video traffic that is sent over Resource Reservation Protocol (RSVP) ATM switched virtual circuits (SVCs). The SVC quality of service (QoS) parameters indicate a small burst (typically 20 percent of the requested IP burst). This situation causes traffic bursts to be dropped even if the traffic bursts are within the specified burst traffic parameters.

  In some cases, the peak cell rate (PCR) and the sustainable cell rate (SCR) may also be lower than what is required for this traffic. The low PCR may cause significant packet loss, video drops, and loss of synchronization between the affected stream and other related streams. The hold queue for the ATM SVC will fill up and remain full for an extended duration.

  Conditions This symptom is observed on Cisco 7200 and 7500 routers when voice or video clients are used to generate a stream of small packets.

  Workaround There is no workaround.

- CSCdy42103

  Symptoms A watchdog timeout may cause a software-forced reload on a router.

  Conditions This symptom is observed on a Cisco 7500 router that is using the Border Gateway Protocol (BGP).

  Workaround There is no workaround.

- CSCdy89098

  Symptoms A router may lock up when it is passing a Voice over IP (VoIP) pass-through call with a third-party device.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(12) and that has Network Address Translation (NAT) configured when version 3 or version 4 H.323 VoIP calls are passing through.

  Workaround There is no workaround.

Miscellaneous

- CSCds81427

  Symptoms When you delete a single subinterface from a 1-port multichannel T3 port adapter (PA-MC-T3), a 2-port multichannel T3 port adapter (PA-MC-2T3), or a 2-port enhanced multichannel T3 port adapter (PA-MC-2T3+), all interfaces may be removed.

  Conditions This symptom is observed on a Cisco 7200 series or Cisco 7500 series router that is running Cisco IOS Release 12.0 S.

  Workaround Do not delete the single subinterface; shut it down instead.

- CSCdu38726

  Symptoms Dynamic Host Configuration Protocol (DHCP) offers cannot be sent through a BRI or dialer interface from a DHCP sever to a DHCP client through an IP Security (IPSec) tunnel.

  Conditions This symptom is observed in a network that has an IPSec tunnel built over a BRI interface. There is a DHCP client and a DHCP server on the opposing ends of the IPSec tunnel. A DHCP request can be sent from the DHCP client to the DHCP server, but a DHCP offer that contains the IP address for the DHCP server cannot be sent back to the DHCP client from the DHCP server through the IPSec tunnel on the BRI or dialer interface.

  Workaround There is no workaround.

- CSCdv00396

  Symptoms A router may reload when a rate limit is unconfigured while the **show interface rate-limit** EXEC command is executed.

  Conditions This symptom is observed on a Cisco router when the rate limit is unconfigured.

  Workaround There is no workaround.

- CSCdv01994

  Symptoms Memory allocation failures (MALLOCFAIL) may be observed on a router after it is reloaded.

  Conditions This symptom is observed on a Cisco 7500 series router.

  Workaround There is no workaround.

- CSCdv21526

  Symptoms When the NetSpeak Internet call waiting functionality is invoked on an H.323 Voice over IP (VoIP) call, the gateway receives an admission confirmation (ACF) that has a destCallSignal address of 0.0.0.0.

Conditions This symptom is observed on a Cisco router when it is configured for RADIUS accounting. The gateway generates a call detail record (CDR) for the initial redirected call leg, and the CDR indicates a cause code of 3 (no route to host). In previous Cisco IOS releases, no CDR was generated for this call leg.

This symptom should not cause billing issues because the CDR indicates a zero call duration. However, users who tabulate the disconnect cause codes for CDRs to diagnose network issues may be incorrectly led to believe that there is a problem in the network. To correct this symptom, the disconnect cause code for the initial redirected leg will be changed to a cause code of 23 (redirection to new destination).

Workaround Ignore the RADIUS CDRs that have a code 3 disconnect cause code and a call duration of zero.

- CSCdv26036

  Symptoms Simple Network Management Protocol (SNMP) queries may fail when Network Management System (NMS) and communities are configured in the docsDevNmAccessTable table.

  Conditions This symptom is observed on a Cisco uBR900 series or Cisco CVA120 series router that is running a Cisco IOS release earlier than Release 12.2.

  Workaround Ensure that there are no interface-specific entries in the docsDevNmAccessTable table; that is, the values of the docsDevNmAccessInterfaces entries should be "0xff." This workaround may prevent you from having interface-specific control on SNMP queries that access the Cisco uBR900 series or Cisco CVA120 series router.

- CSCdv86717

  Symptoms An output queue on an interface may become wedged after a few minutes. The following command output is displayed after the **show interface fast 0/1** EXEC command is entered:

  ```
  FastEthernet0/1 is up, line protocol is up Queueing strategy: fifo Output queue 40/40,
  66826 drops; input queue 0/75, 0 drops
  ```

  Conditions This symptom is observed on a Fast Ethernet or Gigabit Ethernet interface with an i82543 chip that is running Cisco IOS Release 12.2(1).

  Workaround There is no workaround.

- CSCdw01724

  Symptoms Tunnels may become inoperative, and the following traceback message may be displayed:

  ```
  cst: %SYS-3-NULLIDB: Null IDB in ipsendnet -Process= "Crypto HW Proc", ipl= 0, pid=
  65 -Traceback= 606DE4D4 611354B4 6112A494 6112A744 605DD1EC 605DD1D8
  ```

  Conditions This symptom is observed on a Cisco 7200 router.

  Workaround There is no workaround.

- CSCdw16580

  Symptoms A Virtual Private Network (VPN) Routing and Forwarding (VRF) routing table may not be imported to the same provider edge (PE) router even though the PE appears on the Border Gateway Protocol (BGP) Virtual Private Network version 4 (VPNv4) table. When static routes are redistributed to BGP VPNv4 and then imported to another VRF instance on the same PE, not all VRF routes may be installed in the VRF instance that imports them.

  Conditions This symptom is observed on a Cisco 7200 series router that functions as a PE router and that is configured with multiple VRF instances in a Multiprotocol Label Switching (MPLS) VPN environment.

  Workaround There is no workaround.

- CSCdw49806

  Symptoms The Real-Time Protocol (RTP) stream cannot be transferred by the Empty Capability Set feature.

  Conditions This symptom is observed on a Cisco gateway if the openLogicalChannel request and the releaseComplete request are sent from the originating gateway when the RTP transfer process is started between the gateways.

  Workaround There is no workaround.

- CSCdw51589

  Symptoms Inverse Address Resolution Protocol (ARP) fails.

  Conditions This symptom occurs if the **protocol ip in arp** command is entered in virtual circuit (VC) mode on an ATM permanent virtual circuit (PVC) that is configured for inverse ARP operation.

  Workaround Because it is enabled by default, do not use the **protocol ip in arp** command for Inverse ARP operation.

- CSCdw72717

  Symptoms A router may stop passing interzone proxy calls.

  Conditions This symptom is observed on a Cisco 7200 series router that is configured as a gatekeeper.

  Workaround There is no workaround.

- CSCdw74777

  Symptoms The autoinstall over Frame Relay feature does not work.

  Conditions This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(8)T or Release 12.2(10.3)S. During tests of Cisco IOS Release 12.2(10.1)T, the failure is also seen on the Cisco 1600 series and Cisco 2600 series routers.

  Workaround There is no workaround.

- CSCdx00867

  Symptoms You may not be able to make a control connection to an FTP server and you may receive a return acknowledge/push (ack/push) message as part of the initial three-way handshake.

  Conditions This symptom is observed on a Cisco router that is configured with Context-Based Access Control (CBAC).

  Workaround There is no workaround.

- CSCdx17284

  Symptoms A router may reload unexpectedly because of a bus error at PC 0x20d92de, address 0x1b.

  Conditions This symptom is observed on a Cisco 1605 R router that is running the c1600-oy-m firewall image of Cisco IOS Release 12.0(3) and that is used to route traffic between two Class C networks that are configured over the same physical network.

  Workaround Disable fast switching, flow switching, and Cisco Express Forwarding (CEF) switching. Use process switching instead.

- CSCdx17419

  Symptoms The Context-Based Access Control (CBAC) feature of the Cisco IOS Firewall feature set creates dynamic access list entries to allow return traffic from User Datagram Protocol (UDP) sessions that are initiated from within the firewall. Because these access list entries do not handle fragmented traffic, noninitial fragments are dropped.

Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(5).

Workaround Configure a static access list to pass noninitial fragments.

- CSCdx38973

  Symptoms A universal access server may reload.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that is running Cisco IOS Release 12.2(9.4). This symptom occurs when a busyout immediate is performed using the Simple Network Management Protocol (SNMP) on a digital service 0 (DS0) interface that has an active voice call.

  Workaround There is no workaround.

- CSCdx41056

  Symptoms A serial interface that has been previously shut down may be inadvertently brought back up when a router is reloaded.

  Conditions This symptom is observed on a Cisco AS5400 universal access server that has a serial interface.

  Workaround There is no workaround.

- CSCdx42869

  Symptoms More time may be needed to set up some sessions after an access list is configured on a virtual template.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(4)BZ.

  Workaround There is no workaround.

- CSCdx43675

  Symptoms A voice gateway may reload in a debit card stress test.

  Conditions This symptom is observed on a Cisco AS5800 universal access server when the Cisco AS5800 is stress-tested with Toolkit Command Language (TCL) 2.0 scripts.

  Workaround There is no workaround.

- CSCdx45027

  Symptoms A tag does not come up after a flap occurs on an IP-to-Multiprotocol-Label-Switching (MPLS) multivirtual circuit.

  Conditions This symptom is observed in Cisco IOS Release 12.2(10.1)T and Release 12.2(10.3)T1.

  Workaround There is no workaround.

- CSCdx45726

  Symptoms From a remote provider edge (PE) router or from a customer edge (CE) router, you may not be able to ping to IP addresses other than the IP address on the Virtual Routing/Forwarding (VRF) interface on a near-end CE router. The statistics output on the PE router will show the "no_tfib_route" counter being incremented as in the following example:

```
Router# show hardware pxf cpu statistic drop | in tfib|drop

FP drop statistics
no_tfib_route 2762283021 0
bad_drop_code 0 0
master drop count 2923544477.
```

Conditions This symptom is observed on a Cisco 10000 series router after a switchover, when a large number of VRF interfaces are configured and traffic is flowing. The number of routes that are affected varies. This symptom is observed on untagged routes, but not on aggregate routes.

Workaround Enter the **clear ip route vrf** *vpn* * EXEC command.

- CSCdx53140

  Symptoms A forced reload may occur on a router because of a corrupted call detail block (CDB) memory access in Voice Telephony Service Provider (VTSP).

  Conditions This symptom is observed on a Cisco 3810 router when a voice call is started.

  Workaround There is no workaround.

- CSCdx56874

  Symptoms ISDN Layer 2 traffic is processed even after the T1 or E1 controller is shut down.

  Conditions This symptom has been observed on a Cisco AS5300.

  Workaround There is no workaround.

- CSCdx57718

  Symptoms Intermittent IP packet loss may occur in the traffic that is passing via a generic routing encapsulation (GRE) tunnel and that is terminated on a Multilayer Switch Feature Card 2 (MSFC2).

  Conditions This symptom is observed when Cisco Express Forwarding (CEF) is not enabled on the outgoing VLAN interface and the packets are fast switched or process switched. When the outgoing interface of the GRE tunnel is a Packet-over-SONET interface, the symptom does not occur.

  Workaround Enable CEF on the outgoing interface of the GRE tunnel.

- CSCdx59037

  Symptoms A Cisco 3660 router that is running Cisco IOS Release 12.2(6e) or Release 12.2(10.6) and that is using the busyout monitor feature on the voice port may not be able to bring up the trunk connections after the Cisco 3660 is reloaded.

  Conditions This symptom is observed when the **busyout monitor** voice-port configuration command is entered to trigger permanent virtual circuit (PVC) monitoring for connections in a Voice over ATM (VoATM) environment.

  Workaround Perform one of the following workarounds:

  – Configure both the master and slave routers as master routers. This configuration removes the need for the answer mode to be configured on either of the routers.

  – Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the voice port of the router after the router reloads.

- CSCdx64015

  Symptoms A router may reload.

  Conditions This symptom is observed on a Cisco 7200 router with Multilink PPP (MLP) and PPP traffic when Weighted Random Early Detection (WRED) and compression are configured.

  Workaround There is no workaround.

- CSCdx65248

  Symptoms Cisco Express Forwarding (CEF) may be disabled on an ATM OC-3 line card after a memory leak occurs.

  Conditions This symptom is observed on an ATM OC-3 line card.

  Workaround There is no workaround.

- CSCdx66514

  Symptoms The Inverse Multiplexing over ATM (IMA) protocol cannot be brought up between a Cisco router and a vendor-specific switch.

  Conditions This symptom is observed when a vendor-specific switch is used with a Cisco 2600 or Cisco 3600 router. This symptom occurs because Cisco routers do not accept unassigned or idle cells over IMA connections. The vendor-specific switch sends unassigned cells in the IMA frame when there is no user data to send. Unassigned or idle cells are discarded by the ATM interface on the Cisco router, and the IMA protocol fails.

  Workaround There is no workaround.

- CSCdx67721

  Symptoms A segmentation violation (SegV) exception may cause a router to reload unexpectedly.

  Conditions This symptom is observed on a Cisco Catalyst 4224 Access Gateway Switch.

  Workaround There is no workaround.

- CSCdx69748

  Symptoms A router resets itself 5 minutes after reaching the “maintenance state.”

  Conditions This symptom is observed on a Cisco uBR925 cable access router that is running the k8boot image.

  Workaround Set the lease renewal time to a duration that is longer than 5 minutes using the Cisco Network Registrar (CNR). If the lease renewal time is set to a duration of 5 minutes, the Cisco uBR925 may not stay up long enough to allow a new image to be downloaded.

- CSCdx74054

  Symptoms The following two symptoms may be observed when an extended Multiprotocol Label Switching ATM (XTagATM) interface is unconfigured and reconfigured in quick succession by entering the **no interface XTagATM 192** interface configuration command followed by the **interface XTagATM 192** interface configuration command:

  a. The control-VC for the extended tag (XTAG) is not created (addressed by CSCdx88018).

  b. The control-VC may be created, but packets are not transmitted correctly. The interface remains in the “xmit-only” state (addressed by CSCdx74054).

  Conditions This symptom is observed on the XTagATM interface of a Cisco router.

  Workaround Shut down the XTagATM interface first by entering the **shutdown** interface configuration command before entering the **no interface XTagATM 192** interface configuration command followed by the **interface XTagATM 192** interface configuration command. After the **interface XTagATM 192** interface configuration command is entered, enter the **no shutdown** interface configuration command on the XTagATM interface.

- CSCdx77088

  Symptoms A software-forced reload may occur on a router, and the following messages may be displayed:

  ```
  System was restarted by error - a Software forced crash, PC 0x60396E7C at 4500 Software
  (C4500-A3JS-M), Version 12.2(8.1), MAINTENANCE INTERIM SOFTWARE Compiled (current
  version) Image text-base: 0x60008948, data-base: 0x61116000
  ```

  ```
  Stack trace from system failure: FP: 0x618A8458, RA: 0x60396E7C FP: 0x618A8458, RA:
  0x603952F4 FP: 0x618A8480, RA: 0x6039D584 FP: 0x618A84A0, RA: 0x603A0CC8 FP:
  0x618A84C0, RA: 0x60398BDC FP: 0x618A8558, RA: 0x6037E1F0 FP: 0x618A85A0, RA:
  0x6174B1F0
  ```

Conditions This symptom is observed on a Cisco 4500 router that is running Cisco IOS Release 12.2(8.1).

Workaround There is no workaround.

- CSCdx77135

  Symptoms A data terminal ready (DTR) signal in a serial connection does not transition as expected when the pulse-time x command is entered.

  Conditions This symptom is observed on a Cisco 3662 router that has a 1-port serial WAN interface card (WIC-1T), a 2-port serial WAN interface card (WIC-2T), and a 4-port network module (NM-4T) and that is connected to external encryption equipment. The Cisco 3662 may lose the capability to resynchronize with the external encryption equipment because the DTR port adapter does not function as designed when the pulse-time x command is entered.

  Workaround There is no workaround.

- CSCdx78656

  Symptoms When recEive and transMit (E&M) channel-associated signaling (CAS) hairpinned calls are made on a router, the calls disconnect with a 3F cause code (service or option is not available or unspecified) if the **dtmf dnis** option is set in the configuration of the DS0 group.

  Conditions This symptom is observed on a Cisco 2600 series, Cisco 3600 series, or Cisco 3700 series.

  Workaround Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the voice port of the router that is performing the hairpin calls.

- CSCdx83297

  Symptoms A software-forced reload may occur on a Cisco 7206VXR because of I/O memory corruption and redzone overrun.

  Conditions This symptom is observed on a Cisco 7206VXR that is running Cisco IOS Release 12.1(4)XZ6.

  Workaround There is no workaround.

- CSCdx85632

  Symptoms Passive FTP may fail with Context-Based Access Control (CBAC) (with the **ip inspect name** *inspection-name ftp* global configuration command applied to an inside interface) and with Reverse Path Forwarding (RPF) checks enabled.

  Conditions This symptom is observed on a Cisco 1720 router that is running Cisco IOS Release 12.2(8)T4.

  Workaround Turn off the RPF check by issuing the **no ip verify unicast reverse-path** command.

- CSCdx87631

  Symptoms A Cisco gateway card may reload because the I/O memory is corrupted. The following output may be displayed when the **show version** EXEC command is entered after the Cisco gateway card reloads:

  ```
  System returned to ROM by error - a SIGTRAP exception, PC 0x802916DC
  ```

  Conditions This symptom is observed on a Cisco gateway card that is running Cisco IOS Release 12.2(10a).

  Workaround There is no workaround.

- CSCdx88018

  Symptoms The following two symptoms may be observed when an extended Multiprotocol Label Switching (MPLS) ATM (XTagATM) interface is unconfigured and reconfigured in quick succession by entering the **no interface XTagATM 192** interface configuration command followed by the **interface XTagATM 192** interface configuration command:

  a. The control-VC for the extended tag (XTAG) is not created (addressed by CSCdx88018).

  b. The control-VC may be created, but packets are not transmitted correctly. The interface remains in the "xmit-only" state (addressed by CSCdx74054).

  Conditions These symptoms are observed on the XTagATM interface of a Cisco router.

  Workaround Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the XTagATM interface. (The workaround for symptom b is addressed by CSCdx74054.)

- CSCdx89461

  Symptoms An FTP session may pause indefinitely while compressed files such as zip files are transferred.

  Conditions This symptom is observed on a Cisco 3600 series router when a vendor-specific compression protocol is enabled.

  Workaround There is no workaround.

- CSCdx89548

  Symptoms An interface on a Cisco 7500 series channelized T3 port adapter cannot ping a directly connected interface because of adjacency difficulties.

  Conditions The conditions under which these symptoms occur are not known at this time.

  Workaround Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface on the channelized T3 port adapter.

- CSCdx91019

  Symptoms A "connection does not exist" message is displayed when an ATM ping is sent with an incorrect virtual path (VP)/virtual channel (VC) combination in the **ping atm interface atm** *interface vpi vci* **end-loopback** privileged EXEC command. After a VC level (F5) Operation, Administration, and Maintenance (OAM) ping is used, the VP level (F4) OAM ping fails with a "connection does not exist" message.

  Conditions This symptom is observed on a Cisco 6400 Node Switch Processor (NSP) that is running Cisco IOS Release 12.2(2b). This symptom is also observed on the Catalyst LS1010, Catalyst 8510MSR, and Catalyst 8540MSR switch platforms.

  Workaround IP pings and the **ping atm interface atm** *privileged* EXEC command can be used to diagnose the connectivity issues between a Node Route Processor (NRP2) and an NSP.

- CSCdx92804

  Symptoms Fax settings are not removed when the **no voice service voip** global configuration command is entered.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that is running Cisco IOS Release 12.2(7c).

  Workaround First unconfigure the fax setting, and then enter the **no voice service voip** global configuration command.

- CSCdx93120

  Symptoms A Node Switch Processor (NSP) that is attempting to ping a valid or invalid virtual path (VP) may fail and generate the following message:

  ```
  %ATMCORE-3-INTERNAL_ERROR: atmCore_oamRcvPing: No match.
  ```

  Conditions This symptom is observed on a Cisco 6400 NSP that is running Cisco IOS Release 12.2(2b). This symptom occurs when a ping is sent to specific destination ATM switches and is dependent on the format of the loopback cell that is received from the destination ATM switches. Thus, the occurrence of this symptom is difficult to predict and depends on the particular ATM switch implementation of the destination switch.

  Workaround There is no workaround.

- CSCdx94691

  Symptoms If a differentiated services code point (DSCP) default value is configured as one of the matching conditions in an extended access list, the class map may miss packets that are matched by the access list.

  Conditions This symptom is observed on an access list on a Cisco router that has a DSCP value that is configured as one of the matching conditions in an extended access list.

  Workaround Remove the DSCP default value as a matching condition from the access list.

- CSCdx95071

  Symptoms Outgoing ISDN calls may be terminated, and the following error message may be displayed:

  ```
  0x80AF - Resource unavailable, unspecified
  ```

  The “bad” state is indicated in the “curr state” column of the output from the **show voice dsp** EXEC command.

  Conditions This symptom is observed on a Cisco 3640 router that is running Cisco IOS Release 12.2(10a).

  Workaround There is no workaround.

- CSCdx95791

  Symptoms Calls may have only one-way audio. There may be calls for which the digital signal processor (DSP) is not responding to Cisco IOS messages and an additional debug points to the fact that a voice path is available only in one direction.

  Conditions This symptom is observed on a Cisco AS5300.

  Workaround There is no workaround.

- CSCdx96063

  Symptoms Missing Tag Forwarding Information Base (TFIB) entries may be observed after the **clear ip route *** privileged EXEC command is entered.

  Conditions This symptom is observed in a cell-based Multiprotocol Label Switching (MPLS) network while the multiple virtual circuit (VC) feature is enabled.

  Workaround Use the **clear ip route prefix** privileged EXEC command instead of the **clear ip route *** privileged EXEC command.

- CSCdy00247

  Symptoms The modemcap AT command string may be in the input buffer of a line when the line comes up. As a result, this string—rather than actual user data received from the client modem—may be used for character mode authentication.

  Conditions This symptom is observed on a Cisco AS5800 that has autoconfiguration enabled on the modem lines.

  Workaround Enter the **flush-at-activation** command.

  Alternate Workaround Ensure that the modemcap entry that is configured on the line sends an AT command that is no longer than 58 characters.

- CSCdy01077

  Symptoms The following error messages may be displayed on the console port of a Cisco Catalyst 6000 switch:

  ```
  %TFIB-7-SCANSABORTED: TFIB scan not completing. MAC string updated.
  %TFIB-DFC8-7-SCANSABORTED: TFIB scan not completing. MAC string updated. *
  ```

  The messages may continue to be displayed until the Cisco Catalyst 6000 switch is reloaded. The error messages are informational and indicate that an excessive amount of network or line transitions may cause an excessive number of Forwarding Information Base (FIB) scans. Processes that are attempting to converge on the network may cause the Route Processor (RP) and the Switch Processor (SP) CPU utilization to occasionally reach 100 percent.

  Conditions This symptom is observed on a Cisco Catalyst 6000 switch that is running Cisco IOS Release 12.2.

  Workaround There is no workaround.

- CSCdy03361

  Symptoms Packet drops may occur in the Cisco Express Forwarding (CEF) and distributed Cisco Express Forwarding (dCEF) paths after a router is reloaded when a ping is sent (through the router) to the IP address of a directly connected customer edge (CE) router.

  Conditions This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2(6). The CE router in this setup is connected to a Fast Ethernet Virtual Private Network (VPN) routing/forwarding (VRF) dot1q subinterface that has the **mpls netflow egress** interface configuration command configured.

  Workaround The Cisco 7500 series router can ping the IP address of the directly connected CE router and cause the relevant Address Resolution Protocol (ARP) entries to be populated.

  Alternate Workaround A Remove the **mpls netflow egress** interface configuration command from the subinterface.

  Alternate Workaround B Add a static ARP entry for the VRF subinterface by entering the **arp vrf ip mask mac arpa** global configuration command.

  Alternate Workaround C Enter the **clear arp** privileged EXEC command on the destination CE router.

- CSCdy04013

  Symptoms A physical unit (PU) that is connected downstream to a Systems Network Architecture Switching Services (SNASw) router may enter the reset state when another PU connects to it using the same cpname and same IDBLK/IDNUM physical unit identifier. The reset state of the PU is indicated in the output of the **show snasw pu** EXEC command. The problem determination log (PDLOG) will display an “invalid internal state detected” message when this symptom occurs.

Conditions This symptom is observed on a Cisco router. The SNASw router has to be restarted to clear this symptom.

Workaround Use the dyncplen connection type.

- CSCdy04411

  Symptoms Under rare circumstances, a Channelized T3 (CT3) card may reboot because of a bus error and then recover. The router itself does not reboot or reload; just the card by itself.

  Conditions This symptom is observed when the CT3 card is installed on a Cisco AS5850 that is running Cisco IOS Release 12.2(2)XB6.

  Workaround There is no workaround.

- CSCdy04914

  Symptoms A permanent virtual circuit (PVC) does not come up even after an alarm indication signal (AIS) is stopped. This symptom is observed after an AIS is received on the PVC from an ATM network and the PVC configuration is changed.

  Conditions This symptom is observed on a Cisco 7507 router that is configured with Operation, Administration, and Maintenance (OAM) management. To recreate this symptom, the PVC configuration must be changed while the PVC is in the AIS or remote defect indication OAM VC state.

  Workaround Reset the PVC by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCdy05804

  Symptoms If a service output policy map that has Weighted Random Early Detection (WRED) configured is used at a Frame Relay map class and if Frame Relay fragmentation is already configured, the WRED threshold values are different from the default value. Class-based weighted fair queueing (CBWFQ) may be affected by this change in behavior.

  Conditions This symptom is observed on a Cisco router.

  Workaround There is no workaround.

- CSCdy07131

  Symptoms A router may not complete the Dynamic Host Configuration Protocol (DHCP) autoinstall process.

  Conditions This symptom is observed on a Cisco router that does not have a nonvolatile memory (NVM) startup configuration.

  Workaround There is no workaround.

- CSCdy08698

  Symptoms Sessions that have a destination logical unit that is a low entry networking (LEN) control point (CP) downstream from a Systems Network Architecture Switching Services (SNASw) branch network node (BrNN) may fail with a sense code of 087D0001. The LEN CP does not show up in the directory database on the host network node server or on the BrNN.

  Conditions This symptom is observed on a SNASw switch.

  Workaround Add a location statement for the LEN CP to the SNASw configuration.

- CSCdy09165

  Symptoms Security association (SA) traffic may not be passed on certain platforms.

  Conditions This symptom is observed on a Cisco 805 or Cisco 4500 series router after Internet Key Exchange (IKE) is established. This symptom is observed with preshare and Rivest, Shamir, and Adleman (RSA) IKE keys.

  Workaround There is no workaround.

- CSCdy09292

  Symptoms Physical inverse multiplexing over ATM (IMA) ports are not indexed in the IF-MIB.

  Conditions This symptom is observed on a Cisco router that has IMA interfaces. This symptom is resolved in Cisco IOS Release 12.2(3)T but may occur in Cisco IOS Release 12.2(8)T and Release 12.2(10.3)T2.

  The following example of the IF-MIB shows ATM1/IMA0 (index 43), but the interface is not indexed:

```
ifDescr.40 = ATM1/7-aal5 layer
ifDescr.41 = ATM1/7.0-aal5 layer
ifDescr.42 = Null0
ifDescr.43 = ATM1/ima0 <----
ifDescr.44 = ATM1/ima0-atm layer
ifDescr.45 = ATM1/ima0.0-atm subif
ifDescr.46 = ATM1/ima0-aal5 layer
ifDescr.47 = ATM1/ima0.0-aal5 layer
ifDescr.48 = ATM1/ima0.40-atm subif
ifDescr.49 = ATM1/ima0.40-aal5 layer
```

  Workaround There is no workaround.

- CSCdy09595

  Symptoms A Cisco voice gateway may reload unexpectedly when it is booting up.

  Conditions This symptom is observed on a Cisco router that is running a Cisco IOS software image that supports voice.

  Workaround There is no workaround.

- CSCdy09937

  Symptoms After a script connection is configured on a line, the specified chat script should execute when an outbound connection (such as reverse Telnet) is made to that line. The observed behavior is that the chat script does not execute and the reverse Telnet session pauses indefinitely. The following message may be displayed when the **debug modem** EXEC command is enabled:

```
TTY33: cleanup pending. Delaying DTR
```

  Similarly, the EXEC session pauses indefinitely after a “script activation” causes the chat script to be executed on an incoming call.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(10.7)T5 or Release 12.2(4)T1.

  Workaround There is no workaround.

- CSCdy09979

  Symptoms A Route Processor (RP) may reload when traffic engineering (TE) tunnels are configured.

Conditions This symptom is observed on an RP that is running the gsr-p-mz image of Cisco IOS Release 12.0(22.1)S. The reload typically occurs after one or more tunnels are removed by entering the **no interface** *interface-type interface-number* global configuration command.

Workaround Do not remove the tunnel interfaces.

- CSCdy10293

  Symptoms A Versatile Interface Processor (VIP) on a Cisco 7500 series router may run out of memory and generate the following memory allocation (MALLOC) failure messages:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 65556 bytes failed from 0x6010EB8C, alignment
  32 Pool: Processor Free: 173756 Cause: Memory fragmentation Alternate Pool: None Free:
  0 Cause: No Alternate pool
  -Process= "CEF IPC Background", ipl= 0, pid= 31
  ```

  The show process memory section in the output of the **show tech** EXEC command indicates that the Multiprotocol Label Switching (MPLS) Cisco Express Forwarding (CEF) interprocess communication (IPC) background process is holding up a large portion of the memory.

  Conditions This symptom is observed on the VIP of a Cisco 7500 series router.

  Workaround There is no workaround.

- CSCdy10610

  Symptoms The received uncompressed bytes counter in the output of the **show compression** EXEC command is not calculated correctly. The received uncompressed bytes counter should show the number of the received compressed bytes that cannot be decompressed and the number of bytes that have been decompressed.

  Conditions This symptom is observed on a Cisco 3660 router.

  Workaround There is no workaround.

- CSCdy11912

  Symptoms Calls that are placed through a Cisco AS5300 may be disconnected, and the following error message may be displayed:

  ```
  %CSM_VOICE-3-NOTDMCHNL: CSM failed to get a free dsp tdm channel from the DSP Resource
  Manager (DSPRM) to handle an incoming call: Adios ! no tdm timeslot:
  dsprm_tdm_release_channel grave error. (23790)
  ```

  Conditions This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2.

  Workaround Use Cisco IOS Release 12.2 T instead of Release 12.2.

- CSCdy12404

  Symptoms A Cisco router may reload because of a bus error when you download per-user access control lists (ACLs) from a RADIUS server and configure these ACLs for each connection.

  Conditions This symptom is observed on but may not be limited to a Cisco AS5850.

  Workaround Configure static ACLs for each connection.

- CSCdy13167

  Symptoms Interactive voice response (IVR) on a universal access server returns a 0 disconnect cause code.

  Conditions This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(6a) and Tool Command Language (TCL) 2.0.1 and that is configured with IVR.

  Workaround There is no workaround.

- CSCdy14102

  Symptoms If two active lines that are connected to ISDN BRI interfaces on a 4-port ISDN BRI network module (NM-4B-S/T) are unplugged simultaneously, one of the ISDN BRI interfaces may display the Layer 1 status as "DEACTIVATED" when the **show isdn status** EXEC command is entered.

  Conditions This symptom is observed on a Cisco 2600 series router that has a NM-4B-S/T network module and that is running Cisco IOS Release 12.1(16).

  Workaround Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ISDN BRI interface that exhibits this symptom.

- CSCdy15222

  Symptoms A routed bridge encapsulation (RBE) client is allowed to continue using a lease even after the lease has expired if users have statically configured the address to the device before it expires.

  Conditions This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(3.1)T or Release 12.2(2)B. The symptom has also been reproduced in Cisco IOS Release 12.2(11.7)T and Release 12.2(4)B4.

  Workaround Configure the Address Resolution Protocol (ARP) timeout to 50 seconds or fewer.

Caution For a large number of RBE users, this workaround could cause a very high CPU utilization, which makes this workaround unsuitable.

- CSCdy16585

  Symptoms A Dynamic Host Configuration Protocol (DHCP) server jumps to 0.0.0.1 as the next usable IP address after the last IP address in the pool is offered.

  Conditions This symptom is observed if the *high-address* argument in the exclude range is configured as 255.255.255.255 in the **ip dhcp excluded-address** *low-address* [*high-address*] global configuration command.

  Workaround Do not specify 255.255.255.255 as the *high-address* argument in the **ip dhcp excluded-address** *low-address* [*high-address*] global configuration command.

- CSCdy17724

  Symptoms When IP Fast Switching is enabled, disabling IP Flow Switching using the 'no ip route-cache flow' on all interfaces and 'no ip flow ingress' on all subinterfaces does not free the NetFlow main cache.

  Conditions This symptom is observed when IP Flow Switching is configured for the first time on an interface.

  Workaround There is no workaround. This issue was resolved in Release 12.2(13).

- CSCdy18641

  Symptoms A router may reload unexpectedly when a Layer 2 Tunneling Protocol (L2TP) connection is established.

  Conditions This symptom is observed on a Cisco 7401ASR router that is used as a Layer 2 Tunneling Protocol (L2TP) network server (LNS).

  Workaround There is no workaround.

- CSCdy19277

  Symptoms A Systems Network Architecture Switching Services (SNASw) boundary function does not unbind a primary logical unit-secondary logical unit (PLU-SLU) session when a cold activate logical unit (ACTLU) response (RSP) is received. The PLU-SLU session on the downstream physical unit (DSPU) cannot be restarted because the virtual telecommunications access method (VTAM) and SNASw are not in agreement about the state of the PLU-SLU session with the DSPU.

  Conditions This symptom is observed on a SNASw switch. When an old Downstream Physical Unit (DSPU) sends a cold ACTLU RSP to a dependent logical unit requester (DLUR), it indicates that a PLU-SLU session is over and the cold ACTLU response should not be used.

  Workaround Restart SNASw or the DSPU.

- CSCdy20168

  Symptoms A memory leak may be observed at radius_initconfig.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdy20170

  Symptoms Poor fax and voice quality may be observed on a Cisco 7200VXR router that has an enhanced digital voice port adapter (PA-VXC+) or a multiservice interchange (MIX)-enabled port adapter (PA-MCX). This symptom occurs because of clock synchronization issues with the remote PBX or public switched telephone network (PSTN).

  This symptom can be corrected by entering the **frame-clock-select** command to configure the primary clock on the Cisco 7200VXR to avoid frame slips that occur when a clock is unsynchronized.

  Conditions This symptom is observed on a Cisco 7200VXR router that has a PA-VXC+ or PA-MCX port adapter.

  Workaround This symptom can be corrected by entering the **frame-clock-select** command to configure the primary clock on the Cisco 7200VXR to avoid frame slips that occur when a clock is unsynchronized.

- CSCdy22004

  Symptoms A universal access server may reload and display the following message when an on-ramp fax or voice call is received:

  ```
  System returned to ROM by bus error at PC 0x6113DBF4, address 0x518
  ```

  Conditions This symptom is observed on a Cisco AS5350 universal gateway.

  Workaround There is no workaround.

- CSCdy24838

  Symptoms Physical units remain in the Pend Activate Physical Unit (ACTPU) state, and the **show snasw pu** EXEC command shows several downstream physical units (DSPUs) that have the same IDBLK/IDNUM physical unit identifier. The virtual telecommunications access method (VTAM) may be slow to send a response to the Request Activate Physical Unit (REQACTPU), and the DSPU disconnects and reconnects before the response arrives from VTAM. When the DSPU reconnects, Systems Network Architecture (SNA) Switching Services (SNASw) may treat the DSPU as a new DSPU. When VTAM sends the REQACTPU, SNASw may assume that there are two DSPUs with the same name and rejects the request with a 082C 002 sense code.

  Conditions This symptom is observed when the user is waiting for the REQACTPU from the VTAM.

  Workaround There is no workaround.

- CSCdy26487

  Symptoms An E1 interface may report that it is handling more than its maximum bandwidth of 1984 kbps.

  Conditions This symptom is observed on an E1 channel group that is configured with 31 time slots.

  Workaround There is no workaround.

- CSCdy26606

  Symptoms A Versatile Interface Processor (VIP) that has a High-Speed Serial Interface (HSSI) reloads continuously after the router is reloaded.

  Conditions This symptom is observed when the HSSI interface is in the shutdown state and when it is configured for Frame Relay encapsulation while a quality of service (QoS) with priority feature is enabled.

  Workaround Enter the **no shutdown** interface configuration command on the interface or remove the QoS policy before reloading the router.

- CSCdy27052

  Symptoms A router may reload unexpectedly.

  Conditions This symptom is observed on a Cisco 7500 router.

  Workaround There is no workaround.

- CSCdy27150

  Symptoms The Cisco ATA 186 analog telephone adapter may not work correctly with Cisco gateways and Cisco gatekeepers when the Cisco ATA 186 is configured to register both E164 identification (ID) and H.323 ID and if the Cisco ATA 186 is not synchronized to the same Network Time Protocol (NTP) time source to which the Cisco gateways and Cisco gatekeepers are synchronized.

  Conditions This symptom is observed on a Cisco ATA 186 analog telephone adapter that is running Cisco IOS Release 12.2(7b).

  Workaround Synchronize both the gateway and gatekeeper to the same NTP time source or avoid configuring the H.323 ID with the Cisco ATA 186.

- CSCdy28353

  Symptoms An incorrect cause code is received on the E1 R2 side when a gateway receives an admission rejection (ARJ) for a gatekeeper.

  Conditions This symptom is observed on a Cisco AS5300 universal access server.

  Workaround There is no workaround.

- CSCdy29558

  Symptoms A Simple Network Management Protocol (SNMP) query for DS0 entities from the cpmDS0UsageTable object in the CISCO-POP-MGMT-MIB fails over an Engine 1 port that is configured with Channel Associated Signalling (CAS). The DS0 entity (specifically, ds0-group) information is not populated in the MIB table.

  Conditions This symptom is observed on the Cisco AS5300, Cisco AS5350, Cisco AS5400, Cisco AS5800, and Cisco AS5850 platforms when running Cisco IOS Release 12.2(11)T.

  Workaround There is no workaround.

- CSCdy33065

  Symptoms The RADIUS call detail records (CDRs) that are generated for egress legs for channel-associated signaling (CAS) calls do not display the DS0 number for the "cisco-vsa-port-string" and the "cisco-avpair" fields correctly and the fields are always set to 0.

  Conditions This symptom is observed only on Cisco AS5300, Cisco AS5400, and Cisco AS5800 access servers that are running Cisco IOS Release 12.2(11)T. This symptom is observed only with outgoing public switched telephone network (PSTN) calls that are made via CAS.

  Workaround There is no workaround.

- CSCdy33386

  Symptoms The old ATM PVC command does not allow any data to be transmitted on a permanent virtual circuit (PVC).

  Conditions This symptom is observed on a Cisco 3600 series router.

  Workaround Use the new ATM PVC command.

- CSCdy34876

  Symptoms Errors may be observed with a data transfer.

  Conditions This symptom is observed when asynchronous tunneling is done through a 2-port async/sync WAN interface card (WIC-2A/S) on a Cisco 3600 series.

  Workaround There is no workaround.

- CSCdy36274

  Symptoms A hung time slot may be observed on a Cisco voice gateway.

  Conditions This symptom is observed when a call is made after it has just been disconnected in quick succession on the same time slot on a Cisco voice gateway that is running E1 R2 signaling.

  Workaround There is no workaround.

- CSCdy36665

  Symptoms Operation, Administration, and Maintenance (OAM)-managed permanent virtual circuits (PVCs) on a 8-port T1 ATM port adapter with IMA (PA-A3-8T1IMA) or on an 8-port E1 ATM port adapter with IMA (PA-A3-8E1IMA) may not come up as expected.

  Conditions This symptom is observed on a PA-A3-8T1IMA or a PA-A3-8E1IMA of a Cisco 7200 series or Cisco 7500 series that is running Cisco IOS Release 12.2(11.5)T or a later release.

  Workaround There is no workaround.

- CSCdy36952

  Symptoms A router may reload after about 10 hours of run time when a T.38 fax configuration is load tested.

  Conditions This symptom is observed on a Cisco 3640 router when 40 T1 channel-associated signaling (CAS) channels of a T.38 fax configuration on the router are load tested.

  Workaround There is no workaround.

- CSCdy37551

  Symptoms IP connectivity may be lost and a Telnet session to a router may lock up when the **crypto map** *map-name seq-num* **ipsec-isakmp** global configuration command is entered.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2, Release 12.1 E, or Release 12.2(11)T. This symptom is observed when a Telnet session is made to a router over a generic routing encapsulation (GRE)-IP Security (IPSec) tunnel and when a new

crypto map entry is added to an existing crypto map that is already applied to the GRE-IPSec tunnel and the associated physical interface. This symptom affects only the GRE-IPSec tunnel and not the IPSec tunnel.

Workaround Remove the crypto map from the tunnel and the physical interface. Add the new map instance, and reapply the crypto map to the interfaces.

- CSCdy38681

  Symptoms A 1-port ATM Enhanced OC12/STM4 port adapter (PA-A3-OC12) that is configured with multiple Low Latency Queueing (LLQ) streams that are running near peak cell rate (PCR) may drop packets. The output of the **show interfaces** command displays that packets are sent out but no packets are coming in. Input or output packet drops are not displayed.

  Conditions This symptom is observed during a test on a Cisco 7500 series router that is running Cisco IOS Release 12.0(22)S.

  Temporary Workaround Enter the **clear interface** *type number* EXEC command each time the symptom occurs.

- CSCdy38691

  Symptoms A provider edge (PE) headend router that is running Multiprotocol Label Switching (MPLS) and that is connected via a Label Distribution Protocol (LDP) link to a neighboring provider (P) router may reload when one or more interfaces on the P router are unconfigured using the following sequence of commands (all commands are entered):

  a. **no mpls ip** global configuration command
  b. **no mpls ip** interface configuration command
  c. **shutdown** interface configuration command

  Conditions This symptom is observed on LDP neighbors that are connected via label controlled ATM (LC-ATM) interfaces. The symptom may not occur when Tag Distribution Protocol (TDP) is the label signaling protocol.

  Workaround Shut down the LC-ATM interface of the PE headend router before you enter the three above-mentioned configuration commands on the P router.

  Alternate Workaround Do not use all three above-mentioned configuration commands to unconfigure the interface on the P router. Instead, use only the two interface configuration commands, that is, the **no mpls ip** and **shutdown** interface configuration commands.

- CSCdy40192

  Symptoms One-way audio may be observed and packets may be dropped on the serial interface of the outgoing data-link connection identifier (DLCI) on a Cisco 7507 router. The data connectivity slows and eventually stops, after which, no packets are received on the remote router.

  Conditions This symptom is observed on a Cisco 7507 router that has a Versatile Interface Processor (VIP) that is configured for Voice over Frame Relay (VoFR) using the VIP-based Frame Relay Forum implementation agreement for VoFR (FRF.11) and the Frame Relay Forum implementation agreement for VoFR (FRF.12). The Cisco 7507 router is set up for VoFR calls to a remote Cisco 2600 series router that has calls that terminate on an analog phone on a Foreign Exchange Station (FXS) port. The user on the Cisco 7507 can hear the user on the Cisco 2600, but the user on the Cisco 2600 cannot hear anything.

  Workaround There is no workaround.

- CSCdy41326

  Symptoms A Cisco 7500 series may reload because of a bus error and display the following message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
  ```

  This error occurs because only TCP header compression is enabled on a distributed Cisco Express Forwarding (dCEF) multilink bundle interface.

  Conditions This symptom is observed on a Cisco 7500 series that is running Cisco IOS Release 12.2(11.7)T.

  Workaround Ensure that TCP header compression is not enabled on any multilink bundle interface or in any associated authentication, authorization, and accounting (AAA) RADIUS database.

  Alternate Workaround Enter the **ip rtp header-compression iphc-format** interface configuration command to enable both TCP and Real-Time Transport Protocol (RTP) compression.

- CSCdy41507

  Symptoms A router may reload when the Enhanced Interior Gateway Routing Protocol (EIGRP) attempts to establish the neighborhood.

  Conditions This symptom is observed on a Cisco 2600 series that has two serial interfaces that are configured to perform Cisco Express Forwarding (CEF) per-packet load balancing. In the observed setup, EIGRP is running over a generic routing encapsulation (GRE) tunnel and Cisco IOS Release 12.2(11)T is used. This symptom is triggered by recursive routing that is caused by an incorrect EIGRP configuration.

  Workaround Check the routing configuration of the router to remove any triggers that may cause recursive routing to occur.

- CSCdy42349

  This caveat consists of two symptoms, two conditions, and two workarounds.

  Symptoms A A Versatile Interface Processor (VIP) may reload when you enable the **mpls netflow egress** interface configuration command on a dot1q interface.

  Conditions A This symptom is observed on a VIP that is installed in a Cisco 7500 series router that has 802.1q trunking and Virtual Private Network (VPN) configured.

  Workaround A There is no workaround.

  Symptoms B Alignment errors may occur on Multiprotocol Label Switching (MPLS) packets that are traversing the feature path, such as the packets that encounter a service policy.

  Conditions B This symptom is observed on a Cisco 7200 series router that has 802.1q trunking and Virtual Private Network (VPN) configured.

  Workaround B There is no workaround.

- CSCdy43292

  Symptoms A router may fail to provide initial connectivity to customer edge (CE) devices.

  Conditions This symptom is observed on a Cisco 7500 series router that is using Cisco Express Forwarding (CEF) or distributed Cisco Express Forwarding (dCEF) with 802.1q Fast Ethernet and that has the Multiprotocol Label Switching (MPLS) egress NetFlow accounting feature enabled.

  Workaround Ping the CE device from the Cisco 7500, or unconfigure the **mpls netflow egress** interface configuration command.

- CSCdy45129

  Symptoms The Inverse Address Resolution Protocol does not work if the **protocol ip inarp** bundle configuration command is entered in the bundle mode.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(12.2)T1.

  Workaround There is no workaround.

- CSCdy45903

  Symptoms Although a "Disconnect" message enters a Voice over IP (VoIP) network with a Progress Indicator (PI), a gateway in the VoIP network may transmit the "Disconnect" message without the PI and never respond to a subsequent ISDN release with a "Release Complete" message.

  Conditions This symptom is observed in Cisco IOS Release 12.2 in a configuration with two VoIP gateways that both have the **isdn global-disconnect** interface configuration command enabled and that both are connected to a Euro-ISDN PRI signaling system after a call is connected and the "Disconnect" message arrives with a PI information element (IE) that has a value of 8.

  Workaround There is no workaround.

- CSCdy46242

  Symptoms A Cisco 7200 series may reload when an online insertion and removal (OIR) is performed on an Integrated Services Adapter (ISA) crypto engine if the RSA-SIG or RSA-ENCR authentication method is used.

  Conditions This symptom is observed on a Cisco 7200 series that is running Cisco IOS Release 12.2(12).

  Workaround There is no workaround.

- CSCdy47494

  Symptoms A memory leak in the Voice over IP (VoIP) process may cause a router to run out of memory. The amount of memory that is used by VoIP and authentication, authorization, and accounting (AAA) can be verified by entering the **show process memory** EXEC command.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that is running Cisco IOS Release 12.2(10b) and that is configured for VoIP and AAA.

  Workaround There is no workaround.

- CSCdy49716

  Symptoms A router may reload after the following series of commands is entered on the router:

  ```
  clear crypto sa
  clear crypto isa
  term width 0
  show crypto engine configuration
  config terminal
  no service alignment detection
  no service alignment logging
  service alignment detection
  ```

  Conditions This symptom is observed on a Cisco 1700 router that is running Cisco IOS Release 12.2(12).

  Workaround Switch the sequence of the following commands in the configuration:

  ```
  no service alignment detection
  no service alignment logging
  ```

Enter the **no service alignment logging** command before entering the **no service alignment detection** command.

- CSCdy50509

  Symptoms An extended security access control list (ACL) that has the "lt 0" or "gt 65535" keyword should not match any port. However, when you use a Turbo ACL that has the **access-list compiled** global configuration command enabled, the "lt 0" or "gt 65535" keyword will match any port.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround Remove the "lt 0" or "gt 65535" keyword.

- CSCdy51183

  Symptoms A router that is running cell-mode tag switching or Multiprotocol Label Switching (MPLS) on a label controlled ATM (LC-ATM) interface may reload when it receives a more specific prefix for a label mapping or binding than the one that is already allocated. For example, the router may reload when it receives the prefix 10.1.1.0/24 if a binding was already allocated for 10.1.1.1/32 on the basis of the routing entry 10.1.0.0/16.

  Conditions This symptom is observed on an Edge Label Switch Router (ELSR) or Label Switch Controller (LSC).

  Workaround There is no workaround for an ELSR. To prevent an LSC from reloading, disable the headend label virtual circuits (LVCs) by entering the **tag-switching atm disable-headend-vcs** global configuration command.

- CSCdy52437

  Symptoms A priority command may not take effect.

  Conditions This symptom is observed when the priority command is configured in a class in a policy.

  Workaround Remove the class from the policy, and reconfigure the priority command.

- CSCdy52947

  Symptoms A Cisco router that is running the Cisco General Packet Radio Service (GPRS) support node (GGSN) release 1.4 image of Cisco IOS Release 12.2(10a) may reload if a create Packet Data Protocol (PDP) request message is received on an existing PDP context that has a new recovery information element (IE).

  Conditions The Cisco router reloads if the new create request that is received has the same target identifier (TID) but a different recovery IE. This symptom is observed after a PDP context is successfully opened while charging is disabled on the Cisco router.

  Workaround There is no workaround.

- CSCdy53351

  Symptoms A Cisco router that is running Cisco General Packet Radio Service (GPRS) support node (GGSN) release 1.4 software may leak memory if a new create or delete Packet Data Protocol (PDP) request message is received on an existing PDP context that is waiting for a RADIUS and Dynamic Host Configuration Protocol (DHCP) server response.

  Conditions This symptom is observed only if the create or delete PDP request is not a retry request and contains a different GPRS Tunneling Protocol (GTP) sequence number from the earlier request. This symptom is observed if the GGSN is waiting for a response from the RADIUS or DHCP server.

  Workaround There is no workaround.

- CSCdy54337

  Symptoms An interface on a 2-port Fast Ethernet port adapter (PA-2FE) may stop transmitting if this interface or the other interface on the same port adapter goes down or flaps under a heavy traffic load. The interface that stops transmitting may display the following messages:

  ```
  %RSP-3-RESTART: interface FastEthernet3/0/0, not transmitting
  %RSP-3-RESTART: interface FastEthernet3/0/0, output frozen
  %RSP-3-RESTART: cbus complex
  ```

  Conditions This symptom is observed on the PA-2FE on a Cisco 7500 series Versatile Interface Processor 4 (VIP4) that is configured with Fast Ether Channel (FEC). This symptom is observed when the port adapter is carrying a heavy traffic load and when part of the traffic is originating from a port adapter (PA-A3) that is located on the same VIP.

  Workaround There is no workaround.

- CSCdy54364

  Symptoms A Cisco 1751 may reload if the **isdn leased-line bri** global configuration command is configured while one or both of the B channels are active.

  Conditions This symptom is observed on the BRI interface of a Cisco 1751 that is running Cisco IOS Release 12.2(11.3)T1.

  Workaround Shut down the BRI interface before applying the leased line configuration. Place the leased line configuration on the BRI interface only after ensuring that there are no active calls on either of the B channels.

- CSCdy54989

  Symptoms All packets that are sent to a line card are shown as queued up when the **show cef linecard** command is issued.

  Conditions This symptom is observed when the Forwarding Information Base (FIB) is disabled on the line card.

  Workaround Issue the **clear cef linecard** *slot-number* command. If this does not correct the problem, perform an online insertion and removal (OIR) procedure on the affected line card.

- CSCdy56930

  Symptoms Resource management (RM) cells are not generated on an enhanced ATM port adapter (PA-A3) when a switched virtual circuit (SVC) is configured using the available bit rate (ABR) service category.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(11)T under normal use.

  Workaround There is no workaround.

- CSCdy59848

  Symptoms Packets that are switched from an incoming X.21 interface to an E1 channelized interface may not be sent. Packets that are switched the other way around—from an E1 channelized interface to an X.21 interface—are sent.

  Conditions This symptom is observed on a Cisco 7200 series router.

  Workaround There is no workaround.

- CSCdy60455

  Symptoms A Cisco AS5400 times out when it receives an A-5 signal. The timeout occurs because the A-5 signal is not defined in the Indonesia R2 implementation for Cisco AS5xxx platforms.

  Conditions This symptom is observed on a Cisco AS5400 that is running Cisco IOS Release 12.2(2)XB7.

  Workaround There is no workaround.

- CSCdy60539

  Symptoms A Connectionless Network Service (CLNS) route does not come up if a permanent virtual circuit (PVC) uses Switched Multimegabit Data Service (SMDS) encapsulation.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(12.5)T.

  Workaround There is no workaround.

- CSCdy61222

  Symptoms A Cisco router that is running Cisco General Packet Radio Service (GPRS) support node (GGSN) release 1.4 software may leak memory in the I/O buffer if either of the following conditions is present:

  – An error indication message is received on an existing Packet Data Protocol (PDP) context.

  – A delete request is received on a context that is waiting for a RADIUS or Dynamic Host Configuration Protocol (DHCP) server response, and GGSN does not return the delete response.

  Conditions This symptom is observed if the Cisco router that is running serving GPRS support nodes (SGSNs) reboots and loses all PDP contexts, and GGSN continues to send packets on the context without detecting this condition. The delete request may occur if RADIUS or DHCP takes a longer time than expected to respond to the GGSN.

  Workaround There is no workaround.

- CSCdy63803

  Symptoms After a phone is hung up and a “Disconnect” request is received from the private automatic branch exchange (PABX), a the router should respond immediately with a “Release” request to free up the allocated B channel. On a router that is running Cisco IOS Release 12.2(12), the router does not respond to the “Disconnect” request and the B channel is not freed up until the PABX issues a “Release” request after a time out occurs.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(12).

  Workaround There is no workaround.

- CSCdy66541

  Symptoms A loss of connectivity may be observed on an RSETUP High-Performance Routing (HPR) pipe to a vendor-specific open systems adapter.

  Conditions This symptom is observed in a network in which Systems Network Architecture (SNA) switch routers are connected to Catalyst 6500 series switches via Fast Ethernet ports. The SNA switch routers are connected to the vendor-specific open systems adapter via an enterprise extender.

  The virtual telecommunications access method (VTAM) on the vendor-specific open systems adapter terminates the pipe but the SNA switch router does not terminate the pipe. This behavior causes the pipe to enter into an invalid state and prevents information that is sent over the pipe from reaching the VTAM. Consequently, session setup requests will pause indefinitely.

One indication of the presence of the symptom is that there is more than one pipe to the SNA switch router. When the VTAM detects a loss of connectivity, it terminates the pipe and configures a new pipe. The SNA switch router does not terminate the old pipe but does accept the new pipe from the VTAM. When this situation occurs, the output of the **show snasw rtp** command shows that there is more than one pipe to the SNA switch router. You can compare the output of the **show snasw rtp** command on the SNA switch router to the number of pipes to the VTAM.

Workaround There is no workaround.

- CSCdy68974

  Symptoms I/O memory fragmentation occurs with various digital signal processor (DSP) timeout errors causing alarms to be triggered.

  Conditions This symptom is observed on a Cisco AS5300 with Dual Tone Multifrequency (DTMF) path confirmation enabled.

  Workaround There is no workaround.

- CSCdy69079

  Symptoms A leak may occur in small buffers, and the **show buffer** EXEC command shows a very large number of small buffers. If this situation occurs, shared memory routers such as the Cisco 7200 series router will run out of I/O memory and the Cisco 7500 series router will run out of main memory.

  The symptoms are caused by a buffer leak that occurs when a multicast packet cannot be sent.

  Conditions These symptom are observed on a router that has Virtual Private Network routing/forwarding (VRF) instances configured that are Multiprotocol Label Switching (MPLS) multicast enabled.

  Workaround Eliminate the reason why a multicast packet cannot be sent. Ensure that the MPLS multicast peering loopback interface is configured for Protocol Independent Multicast (PIM), that all the appropriate interfaces are configured for PIM, and that PIM adjacencies are formed.

- CSCdy73244

  Symptoms Guarantees may not be achieved for some classes for a certain combination of bandwidth assignments within a service policy.

  Conditions This symptom is observed when you use the following bandwidth allocation: class 1, 8 kbps; class 2 64 kbps; class 3 16 kbps; class 4 14 kbps; parent class, 120 kbps.

  Workaround Sightly adjust the bandwidth of one of the classes. In the above example, changing class 3 to 14 kbps or class 4 to 16 kbps would solve the situation.

- CSCdy75210

  Symptoms A Cisco Gateway General Packet Radio Service (GPRS) support node (GGSN) may send attributes 42 and 43 twice in an accounting stop request.

  Conditions This symptom is observed when the **aaa accounting update periodic** *number* global configuration command is enabled.

  Workaround There is no workaround.

- CSCdy75466

  Symptoms When a Cisco AS5400 is cold booted (that is, when the Cisco AS5400 is powered off and then on again), the relevant Simple Network Management Protocol (SNMP) coldStart trap is not sent.

  Conditions This symptom is observed on a Cisco AS5400 that is running Cisco IOS Release 12.2, Release 12.2(11)T, or Release 12.2(2)XB8.

  Workaround There is no workaround.

- CSCdy75605

  Symptoms Label Distribution Protocol (LDP)/Tag Distribution Protocol (TDP) sessions may drop under heavy traffic.

  Conditions This symptom is observed when control virtual circuits (VCs) are created but label virtual circuits (LVCs) are not.

  Workaround Stop the traffic until all the LVCs come up and the label controlled ATM (LC-ATM) link stabilizes.

- CSCdy76557

  Symptoms A Cisco Gateway General Packet Radio Service (GPRS) support node (GGSN) may queue up “create requests” and RADIUS messages in the input buffer, may run out of I/O memory, and may reload.

  Conditions This symptom is observed on a GGSN that is running Release 1.4 when the RADIUS server is down and a large number of “create requests” are sent to the GGSN and require RADIUS authentication.

  Workaround There is no workaround.

- CSCdy76986

  Symptoms Distributed switching may not function for packets.

  Conditions This symptom is observed on a distributed multilink interface on a Cisco 7500 series router that is running Cisco IOS Release 12.0(22.4)S1.

  Workaround There is no workaround.

- CSCdy78290

  Symptoms An E1 controller that is configured as unframed via the **channel-group** *number* **unframed** configuration command may generate many path code violations, which are displayed in the output of the **show controllers e1** command.

  Conditions This symptom is observed on an E1 controller of an 8-port multichannel E1 port adapter (PA-MC-8E1) that is installed in a Route Switch Processor (RSP).

  Workaround There is no workaround.

- CSCdy89255

  Symptoms You may not be able to apply more than one input service policy to a Frame Relay subinterface. When you attempt to add a second input service policy, the following message may be generated:

  ```
  A flat policy can be attached to only one sub-interface/pvc. Remove the flat policy
  and retry this command.
  ```

  Conditions This symptom is observed in Cisco IOS Release 12.2(11.4) and Release 12.2(12).

  Workaround There is no workaround.

- CSCdz02391

  Symptoms When the Music on Hold feature sends a music stream, a gateway may not handle traffic properly, causing high CPU utilization, which may affect voice quality.

  Conditions This symptom is observed when a call is made through an H.323 gateway to a Cisco CallManager IP phone and, on the IP phone, the caller is placed on hold. At this point, a Music on Hold stream is sent to the H.323 gateway.

  Although the music is played to caller on the public switched telephone network (PSTN) side, the gateway does not handle the traffic properly and causes the CPU utilization to increase significantly, which, in turn, affects voice quality when a high number of calls are active through the gateway and multiple calls are placed on hold.

  The output of the **show ip traffic** EXEC command displays a rapidly increasing "UDP No Port" counter:

  ```
  UDP statistics:
   Rcvd: 742550 total, 0 checksum errors, 742188 no port
   Sent: 363 total, 0 forwarded broadcasts
  ```

  The output of the **debug ip error** command shows the packets that are causing the "UDP No Port" counter to increment:

  ```
  *IP: s=192.168.0.2 (DSP0), d=0.0.0.0, len 200, dispose udp.noport
  *IP: s=192.168.0.2 (DSP0), d=0.0.0.0, len 200, dispose udp.noport
  ```

  Workaround Disable the Music on Hold feature in the Cisco CallManager for the gateway.

- CSCdz05759

  Symptoms A configuration may be rejected when you load a Cisco IOS software image that supports only the configuration of a police action in terms of numerical data (0 through 64) but not in terms of alphanumerical data (af11, af12, and so on).

  Conditions This symptom is observed when you enter the **policy conform-action set-dscp-transmit** *new-dscp* policy-map configuration command and the *new-dscp* argument has an alphanumerical value.

  Workaround Reconfigure the **policy conform-action set-dscp-transmit** *new-dscp* policy-map configuration command so that *new-dscp* argument has a numerical value.

- CSCdz08348

  Symptoms The redistribution of unicast routes into Distance Vector Multicast Routing Protocol (DVMRP) may not function properly.

  Conditions This symptom is observed when you use the **ip dvmrp metric** *metric* **list** *access-list-number* interface configuration command. This command should allow all unicast routes that are allowed by the value of the *access-list-number* argument to be redistributed with the value of the *metric* argument, but only connected routes are advertised.

  Workaround Explicitly configure the unicast routing protocols that must be advertised, as in the following examples:

  ip dvmrp metric *metric* **list eigrp**

  ip dvmrp metric *metric* **list ospf**

- CSCdz10787

  Symptoms When a label switching router (LSR) reroutes some destinations and selects another interface, the upstream LSR for these destinations may lose the headend label bindings for them.

Conditions This symptom is observed in a Multiprotocol Label Switching (MPLS) ATM network when Intermediate System-to-Intermediate System (IS-IS) is used as the routing protocol.

Temporary Workaround Enter the **clear ip route** *network* EXEC command for the affected destinations until the symptom occurs again.

- CSCin08011

  Symptoms "Voice-tdm connect fail" and "ts-busy" messages may be displayed when digital signal processors (DSPs) are reset while there are ongoing PRI calls.

  Conditions These symptoms are observed on a Cisco router when a DSP is reset while there are ongoing PRI calls. All successive calls cannot be established after this symptom occurs.

  Workaround Terminate the calls, and reset or reconfigure the PRI group.

- CSCin11657

  Symptoms A software-forced reload may occur on a router.

  Conditions This symptom is observed on a Cisco 3640 router when a Simple Resource Coordination Protocol (SRCP) audit gateway (AUGW) with F:PP is sent.

  Workaround There is no workaround.

- CSCin12007

  Symptoms An inverse multiplexing over ATM (IMA) interface does not come back up after it is unconfigured and reconfigured.

  Conditions This symptom is observed when an IMA interface is connected back to back with an advanced integration module (AIM)-based ATM interface that is installed on a Cisco router.

  Workaround Reload the router that has the IMA interface without the ATM configurations in the startup configuration, and reconfigure the IMA interface.

- CSCin14464

  Symptoms A router may pause indefinitely.

  Conditions This symptom is observed on a Cisco 4500 series router when multiple configurations followed by unconfigurations of encapsulations have been done and the switching modes have been changed and when traffic is sent between ATM and Channelized T1 (CT1) interfaces while static routers are configured.

  Workaround There is no workaround.

- CSCin14598

  Symptoms A router may reload when a channel-associated signaling (CAS) is unconfigured on an E1 controller.

  Conditions This symptom is observed on an E1 controller on a Cisco 3640 router that has a digital modem network module (NM-DM).

  Workaround There is no workaround.

- CSCin14762

  Symptoms A router may exhaust its memory and reload.

  Conditions This symptom is observed after a heavy stress load of H.323 calls in which each successful H.323 call causes a small amount of memory to leak.

  Workaround There is no workaround.

- CSCin15491

  Symptoms The H.323 ubr920-k9o3v7y5-mz image is too large to fit in the Flash memory.

Conditions This symptom is observed on a Cisco uBR924 router that is running Cisco IOS Release 12.2(11.8b) and that has a Flash memory size of 4,063,232 bytes.

Workaround There is no workaround.

- CSCin15718

  Symptoms A universal access server may reload when the **clear interface se0:23** EXEC command is entered.

  Conditions This symptom is observed on when ISDN digital calls are made on a Cisco AS5300 universal access server.

  Workaround There is no workaround.

- CSCin16896

  Symptoms A router (router A) may reload if two protocol IP commands are entered in the bundle mode on the router and if the peer router (router B) has Address Resolution Protocol (ARP) enabled.

  Conditions This symptom is observed on a Cisco 7200 router that has ARP enabled.

  Workaround There is no workaround.

- CSCin18414

  Symptoms A Cisco 6400 Node Route Processor (NRP) may not boot properly from Flash memory.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCin20988

  Symptoms A Cisco uBR900 series router may reload.

  Conditions This symptom is observed when a configuration file contains an invalid object identifier (OID).

  Workaround There is no workaround.

- CSCin21199

  Symptoms Spurious memory accesses may occur during the bootup process of a Cisco 7200 series router, or the router may reload during the bootup process.

  Conditions This symptom is observed on a Cisco 7200 series router that is configured with an enhanced 8-port multichannel T1/E1 PRI port adapter (PA-MC-8TE1+) configured in T1 mode and that is configured with a 2-port multichannel T1 port adapter (PA-MC-2T1), a 4-port multichannel T1 port adapter (PA-MC-4T1), or an 8-port multichannel T1 port adapter (PA-MC-8T1).

  Workaround There is no workaround.

- CSCin21761

  Symptoms A Cisco Gateway General Packet Radio Service (GPRS) support node (GGSN) may reload because of a watchdog timeout.

  Conditions This symptom is observed on a GGSN that is running Release 1.4 in Cisco IOS Release 12.2(10a) when the following specific race condition occurs:

  During the Protocol Data Packet (PDP) cleanup process, after the purge timer has stopped but before the PDP is actually freed, if the GGSN receives a “T-PDU” in the fast switching path, the cleanup process is preempted and the purge timer is restarted.

  Workaround Disable fast switching using the **no gprs fastswitch** interface configuration command under the GPRS Tunneling Protocol (GTP) virtual template.

- CSCuk35313

  Symptoms A Cisco 12000 series 8-port Packet-over-SONET OC-3c/STM-1 line card may reload.

  Conditions This symptom is observed when the encapsulation type of one of the interfaces of the line card is set to Frame Relay.

  Workaround There is no workaround.

- CSCuk37305

  Symptoms Wen you specify a non-IP-version-4 (non-IPv4) access list name in the **clear access-list counters** *access-list-name* EXEC command, the router may reload.

  Conditions This symptom is observed only with non-IPv4 access list names, such as Internetwork Packet Exchange (IPX) or IP-version-6 (IPv6) access list names.

  Workaround Enter the **clear access-list counters** EXEC command without supplying a name. Doing so will clear all access lists.

- CSCuk37499

  Symptoms IP header compression may stop compressing frames. This situation may lead to bandwidth starvation and congestion on an associated interface.

  Conditions This symptom is observed when IP header compression attempts to compress a mix of both User Datagram Protocol (UDP) traffic and Real-Time Transport Protocol (RTP) traffic.

  Workaround There is no workaround.

- CSCuk38052

  Symptoms The **neighbor** *ip-address* **capability** router configuration command or the **neighbor** *ip-address* **send-label** router configuration command cannot be configured.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(12.10)T1.

  Workaround There is no workaround.

Novell IPX, XNS, and Apollo Domain

- CSCdv33639

  Symptoms On a router, the following message is displayed:

  ```
  %IPX-3-TOOMANYNETS: Too many networks
  ```

  Conditions This symptom is observed if the number of interfaces that are running the Internetwork Packet Exchange (IPX) protocol exceeds 200. This combination may include a variety of interfaces that are running the Routing Information Protocol (RIP), the Enhanced Interior Gateway Routing Protocol (EIGRP), or the NetWare Link Services Protocol (NLSP). However, if an interface is running both RIP and EIGRP simultaneously, it is considered to be running two protocols instead of one. This means that the 200 limit would be reached if there are 100 interfaces running both RIP and EIGRP.

  Workaround On an interface that is running both EIGRP and RIP, remove either one of the two protocols. Enter the **no network** *network-number* DHCP pool configuration command immediately after the **ipx router rip** global configuration command in the startup-config file of the router where the interface is installed.

- CSCdw10651

  Symptoms With a misconfiguration, the Internetwork Packet Exchange (IPX) Enhanced Interior Gateway Routing Protocol (EIGRP) may cause an interface hold queue to remain wedged at 76/75.

  Conditions This condition occurs because a peer or neighbor is sending the EIGRP one autonomous system number and a neighbor is not getting rid of the autonomous system number because the number exists on the router, but is not used anywhere on the network.

  Workaround Ensure that the peers and the neighbors share the same autonomous system number.

Protocol Translation

- CSCdw83922

  Symptoms A router may reload with a bus error at a null point.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.1(6) or Release 12.1(9) and that is configured for protocol translation.

  Workaround There is no workaround.

  For further information about bus errors, refer to the *Troubleshooting Bus Error Crashes* document at the following location:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml

Wide-Area Networking

- CSCdv36427

  Symptoms A router that is functioning as a Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) may reload.

  Conditions This symptom is observed when L2TP tunnels are created and deleted.

  Workaround There is no workaround.

- CSCdw83920

  Symptoms An incorrect rem_addr RADIUS attribute value may be obtained when a call collision occurs.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(6) and that has callback, ISDN, and RADIUS authentication configured.

  Workaround There is no workaround.

- CSCdw87830

  Symptoms If you copy the configuration to the running configuration using TFTP, not all of the multilink bundles may transition into the “Up” state.

  Conditions This symptom is observed on a Cisco 10000 series router that has a configuration with many multilink bundles.

  Workaround There is no workaround.

- CSCdx12421

  Symptoms When the name information is sent on a vendor-specific switch using a display information element (IE), the first character of the name may be stripped. For example, "John Smith" may be displayed as "ohn Smith."

  Conditions This symptom is observed if both the vendor-specific switch and the router are configured with the Digital Multiplex System (DMS 100) protocol. This symptom is observed if the router does not send the first octet of the display IE as 0xB1 (which is part of the DMS 100 protocol).

  Workaround Insert a space before the first character of the name information display on the system that originates the call. Alternately, the ISDN circuit that is connected to the vendor-specific switch can be configured so that it is controlled by the Cisco Call Manager.

- CSCdx47905

  Symptoms A router may reload if PRI group time slots are partially unconfigured. The entire PRI group configuration is removed from the controller if the **no pri-group** controller configuration command is issued.

  Conditions These symptoms are observed on a Cisco router after the **no pri-group** controller configuration command is issued. Currently ISDN does not support partial unconfiguration of a PRI group.

  Workaround There is no workaround.

- CSCdx65102

  Symptoms A router may reload unexpectedly. The following message may be displayed when the **show version** EXEC command is entered:

  ```
  System returned to ROM by bus error at PC 0x604B9720, address 0xFFFFFFFF
  ```

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(8)T.

  Workaround There is no workaround.

- CSCdx73284

  Symptoms A universal access server may reload when you enter the **no encapsulation frame-relay** interface configuration command on a dialer interface.

  Conditions This symptom is observed on but may not be limited to a Cisco AS5300.

  Workaround There is no workaround.

- CSCdx86538

  Symptoms After a dialer watch connects a call successfully on a PRI, the dialer watch is not able to reconnect a call if the call disconnects because a PRI physical layer has gone down.

  Conditions This symptom is observed on a dialer watch of a Cisco 3600 router that is running Cisco IOS Release 12.2(10). This symptom is not related to the symptoms described in CSCdt60346 and affects only a PRI.

  Workaround Manually ping the remote site, or reboot the router.

- CSCdx90988

  Symptoms A leak with the ISDN process may be observed on a router after about three days. The router reloads because of a lack of memory resources after about 14 days.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(10).

  Workaround Reboot the router at a time when there is low traffic.

- CSCdx94362

  Symptoms The last digit of the calling number is missing in the ISDN Q.931 setup message on a terminating gateway.

  Conditions This symptom is observed on a Cisco AS5300 that is used as a terminating gateway and that is running Cisco IOS Release 12.2(2).

  Workaround There is no workaround.

- CSCdy01448

  Symptoms A memory access violation may be observed on a router when a manual ISDN call is made.

  Conditions This symptom is observed on a Cisco 800 series router that is running Cisco IOS Release 12.2(10a).

  Workaround Remove the **dialer redial interval** interface configuration command from the configuration.

- CSCdy05291

  Symptoms All calls on a Non-Facility Associated Signaling (NFAS) T1 PRI may fail. If the backup D channel is in service, the gateway sends an incorrect channel ID in the call_proc message.

  Conditions This symptom is observed on an NFAS T1 PRI that has a backup D channel.

  Workaround There is no workaround.

- CSCdy10651

  Symptoms Spurious memory access may be observed in the address 0x5C.

  Conditions This symptom is observed on a Cisco 7200VXR that is running Cisco IOS Release 12.2(10a) and that is configured to finish Point-to-Point Tunneling Protocol (PPTP) tunnels.

  Workaround There is no workaround.

- CSCdy16126

  Symptoms Frame Relay switching does not work on a router when distributed Cisco Express Forwarding (CEF) is configured.

  Conditions This symptom is observed if a switched data-link connection identifier (DLCI) is configured directly on a Local Management Interface (LMI) DTE interface on a Cisco 7500 router that has distributed Cisco Express Forwarding (DCEF) configured by entering the **frame-relay interface-dlci** *dlci* interface configuration command.

  This symptom does not occur with an LMI DCE or a Network Node Interface (NNI).

  Workaround Use the **frame-relay route** interface configuration command on the DTE instead of the **frame-relay interface-dlci** *dlci* interface configuration command.

- CSCdy16633

  Symptoms A Cisco router may reload during the Multilink PPP (MLPPP) process.

  Conditions This symptom is observed when the MLPPP is trying to bundle ISDN dial-up connections. The reload occurs when interfaces that belong to the bundle are brought up and down.

  Workaround There is no workaround.

- CSCdy17772

  Symptoms A Voice over IP (VoIP) connection does not pass the Advice of Charge at the end of the call (AOC-E) facility information element (IE) transparently when the AOC-E facility IE is included with a progress indicator in the DISCONNECT message.

Conditions This symptom is observed when the progress indicator IE and a facility IE are part of a DISCONNECT message.

Workaround There is no workaround.

- CSCdy18614

  Symptoms The ISDN process may be terminated on a BRI interface when the first call is made.

  Conditions This symptom is observed on a 5ESS BRI interface that is configured for the 5ESS switch type on a Cisco router that is running Cisco IOS Release 12.2 T. These symptoms are observed only when service profile identifiers (SPIDs) are used on the 5ESS BRI interface.

  Workaround Clear the BRI interface after the router is reloaded before attempting to make any calls.

- CSCdy18949

  Symptoms An ISDN BRI interface does not use the T302 timer as an interdigit timer.

  Conditions This symptom is observed only with voice calls on an ISDN BRI interface that is configured for overlap receiving on a Cisco router that is running Cisco IOS Release 12.2(6e). This symptom does not affect modem or data calls. The inbound dial peer for the voice call does not have the **direct-inward-dial string** dial-peer configuration command configured.

  Workaround There is no workaround.

- CSCdy19427

  Symptoms A call will eventually be disconnected with the incorrect cause code of 0; this cause code is propagated back through the network to the originating side.

  Conditions This symptom is observed on a Cisco AS5xx0 that is running Cisco IOS Release 12.2(10.7)T6, if an egress call is received while the Redundant Link Manager (RLM) is going down.

  Workaround There is no workaround.

- CSCdy23678

  Symptoms After a TCP connection is terminated, the TCP transmissions that are sent by a router are corrupted. The last 6 bytes of the IP header are duplicated in the packet and appear as the first 6 bytes of the TCP header.

  Conditions This symptom is observed on the outgoing interface of a Cisco router that is running Multilink PPP (MLP).

  Workaround Disable MLP.

- CSCdy24524

  Symptoms A router may reload if the **isdn leased-line** global configuration command is configured on a BRI interface that is in the shutdown state.

  Conditions This symptom is observed of a BRI interface on a Cisco router.

  Workaround Do not put the BRI interface into the shutdown state before the **isdn leased-line** global configuration command is configured.

- CSCdy27625

  Symptoms An incorrect interface may be used to send a call.

  Conditions This symptom is observed when two PRI groups are configured on two Digital Subscriber Line (DSL) interfaces, you unconfigure the PRI groups, and you then configure the PRI groups in reverse order. In this situation, the call setup process selects the incorrect interface to send a call.

  Workaround Unconfigure and reconfigure PRI groups in the same order.

- CSCdy28895

  Symptoms A point-to-point subinterface may change to a down state when the switched virtual circuit (SVC) that is configured under the subinterface is deleted.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround Enter the **no shutdown** interface configuration command on the affected subinterface.

- CSCdy33187

  Symptoms Fragmentation may not work normally for multicast traffic. An incorrect header may be used when the router runs an application that replicates and retransmits a packet.

  Conditions This symptom is observed on a Cisco 7200 router.

  Workaround There is no workaround.

- CSCdy38939

  Symptoms A universal access server may reload because of a memory corruption.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that is running Cisco IOS Release 12.1, Release 12.2, or Release 12.2(2)XB. The memory corruption occurs only on a virtual private dial-up network (VPDN) network access server (NAS) when Layer 2 Forwarding (L2F)-encapsulated IP packets are reencapsulated in another L2F tunnel (VPDN packets that are switched using the Stack Group Bidding Protocol (SGBP) in a multichassis-Multilink PPP [MLP] environment).

  Workaround Use the **sgbp protocol l2tp** global configuration command to configure the router to use the Layer 2 Tunneling Protocol (L2TP) as the encapsulation protocol for packets that are forwarded by SGBP.

- CSCdy50020

  Symptoms PPP keepalives that are sourced from a customer premises equipment (CPE) are not passed from a Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) to an L2TP network server (LNS). The missing PPP keepalives may cause the L2TP virtual private dial-up network (VPDN) connection to flap on the CPE.

  Conditions This symptom is observed on a Cisco 7200 router that is running Cisco IOS Release 12.2(10).

  Workaround There is no workaround.

- CSCdy51304

  Symptoms A Cisco 2651 router may not respond to voice calls that come in through a BRI voice interface card (VIC-BRI) and may never generate the dial tone for calling party.

  Conditions This symptom is observed on a Cisco 2651 router that is running Cisco IOS Release 12.2(11)T or a later release in a non-Direct-Inward-Dial (DID) configuration when the incoming call is a public switched telephone network (PSTN) ISDN call.

  Workaround There is no workaround.

- CSCdy54261

  Symptoms A PBX may not support a very large Flow Admission Control (FAC) information element (IE).

  Conditions This symptom is observed when Cisco IOS Release 12.2 T is internetworking with Release 12.2 and you send ISDN User Part (ISUP) Generic Transparent Descriptor (GTD) data from a Voice over IP (VoIP) cloud to an ISDN cloud. This symptom occurs because Release 12.2 does not support very large FAC IEs.

  Workaround There is no workaround.

- CSCdy56616

  Symptoms Disabling the **frame-relay interface-dlci** interface configuration command on an interface while traffic is passing through a permanent virtual circuit (PVC) on the same interface may cause a router to reload.

  Conditions This symptom is observed only on a Cisco 7200 series router.

  Workaround Disable IP fast switching.

- CSCdy64103

  Symptoms The idle timer that is associated with a switched virtual circuit (SVC) may time out even when there is traffic flowing across the circuit, and the idle timer may not be reset.

  Conditions These symptoms are observed when packets are (turbo or process) switched via Cisco Express Forwarding (CEF).

  Workaround Set a large value for the idle timer.

  Alternate Workaround Force legacy fast switching by disabling CEF.

- CSCdy75410

  Symptoms When the primary Non-Facility Associated Signaling (NFAS) member fails, all calls in an NFAS group may disconnect even when the backup NFAS member becomes active.

  Conditions This symptom is observed when the primary NFAS member fails.

  Workaround There is no workaround.

- CSCdy81968

  Symptoms A Cisco 2620 router may reload with a signal trap (Sigtrap) exception.

  Conditions This symptom is observed on a Cisco 2620 router that is running the c2600-is-mz image of Cisco IOS Release 12.2(11)T and that is configured with an 8-port ISDN BRI network module (NM-8B) when four 64-Kb BRI channels are connected.

  Workaround There is no workaround.

- CSCdy84833

  Symptoms ISUP-to-ISUP calls may fail because the terminating gateway creates an extended facility information element (IE) that is out of order.

  Conditions This symptom is observed when a Cisco router that is running Cisco IOS Release 12.2(11)T1 or Release 12.2(11)T2 is configured for a Cisco SS7 Interconnect for Voice Gateways Solution that depends on ISDN User Part (ISUP) transparency.

  Workaround There is no workaround.

- CSCdz04606

  Symptoms A 128-k leased line may go up to only 64 k on a Cisco 1600 series router and may not come up at all on a Cisco 1700 series router.

  Conditions These symptoms are observed when you configure an ISDN BRI interface as a 128-k leased line on a Cisco 1600 series or Cisco 1700 series router and you reload the router to enable the change to take effect.

  Workaround There is no workaround.

- CSCdz17963

  Symptoms A Cisco 2600 series or Cisco 3600 series router that is configured with a Multiflex Trunk (MFT) voice/WAN interface card (VWIC) that is installed in a Fast Ethernet (FE) combo network module (NM) may lose connectivity on port 0 of the MFT VWIC in slot 1 of the FE combo NM. This symptom does not occur on slot 0 of the FE combo NM.

  Conditions This symptom is observed on a Cisco 2600 series or Cisco 3600 series router that is running Cisco IOS Release 12.2(12.4)T or a later release.

  Workaround There is no workaround.

- CSCin07365

  Symptoms A router may reload when you enter the **show queueing interface** privileged EXEC command.

  Conditions This symptom is observed on a router that is functioning as a Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) when there is a lot of downstream data traffic from an L2TP network server (LNS) via the LAC to a client and occurs when Cisco Express Forwarding (CEF), fast switching, or process switching is enabled.

  Workaround There is no workaround.

- CSCin10546

  Symptoms Errors may occur when an ISDN call is placed.

  Conditions This symptom is observed on various Cisco IOS platforms:

  - For the majority of the platforms, the errors consist of spurious memory accesses, which are displayed in the output of the **show alignment** privileged EXEC command.
  - On a Cisco 800 series router, memory protection violations occur.
  - A Cisco 1600 series router unexpectedly reloads.

  Workaround There is no workaround.

- CSCuk36585

  Symptoms A gateway that has an ISDN PRI interface does not use T301 as an interdigit timer.

  Conditions This symptom is observed on a Cisco gateway that is running Cisco IOS Release 12.2(6g) and that has an ISDN PRI interface that is configured for overlap receiving.

  Workaround There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(12m)

Cisco IOS Release 12.2(12m) is a rebuild release for Cisco IOS Release 12.2(12). The caveats in this section are resolved in Cisco IOS Release 12.2(12m) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms: A description of what is observed when the caveat occurs.
- Conditions: The conditions under which the caveat has been known to occur.
- Workaround: Solutions, if available, to counteract the caveat.

IP Routing Protocols

- CSCeh13489

  Symptoms: A router may reset its Border Gateway Protocol (BGP) session.

  Conditions: This symptom is observed when a Cisco router that peers with other routers receives an Autonomous System (AS) path with a length that is equal to or greater than 255.

  Workaround: Configure the **bgp maxas limit** command in such as way that the maximum length of the AS path is a value below 255. When the router receives an update with an excessive AS path value, the prefix is rejected and recorded the event in the log.

Miscellaneous

- CSCei61732

  Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.

  Cisco has made free software available that includes the additional integrity checks for affected customers.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml.

Resolved Caveats—Cisco IOS Release 12.2(12l)

Cisco IOS Release 12.2(12l) is a rebuild release for Cisco IOS Release 12.2(12). The caveats in this section are resolved in Cisco IOS Release 12.2(12l) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms: A description of what is observed when the caveat occurs.
- Conditions: The conditions under which the caveat has been known to occur.
- Workaround: Solutions, if available, to counteract the caveat.

Basic System Services

- CSCed65285

  Certain release trains of Cisco Internetwork Operating System (IOS), when configured to use the IOS Secure Shell (SSH) server in combination with Terminal Access Controller Access Control System Plus (TACACS+) as a means to perform remote management tasks on IOS devices, may contain two vulnerabilities that can potentially cause IOS devices to exhaust resources and reload. Repeated exploitation of these vulnerabilities can result in a Denial of Service (DoS) condition. Use of SSH with Remote Authentication Dial In User Service (RADIUS) is not affected by these vulnerabilities.

  Cisco has made free software available to address these vulnerabilities for all affected customers. There are workarounds available to mitigate the effects of the vulnerability (see the "Workarounds" section of the full advisory for details.)

  This advisory will be posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20050406-ssh.shtml

IP Routing Protocols

- CSCef60659

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at:
  http://www.cpni.gov.uk/docs/re-20050412-00303.pdf

- CSCin31057

  Symptoms: A router may reload when a subinterface with a certain configuration is deleted.

  Conditions: This symptom is observed on a Cisco router that has multicast and the Hot Standby Routing Protocol (HSRP) configured.

  Workaround: Remove the multicast configuration before deleting the subinterface.

- CSCsa59600

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

Miscellaneous

- CSCef44225

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf.

- CSCef44699

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf

TCP/IP Host-Mode Services

- CSCed78149

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled "ICMP Attacks Against TCP" (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP "hard" error messages
  2. Attacks that use ICMP "fragmentation needed and Don't Fragment (DF) bit set" messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP "source quench" messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.cpni.gov.uk/docs/re-20050412-00303.pdf

Resolved Caveats—Cisco IOS Release 12.2(12k)

Cisco IOS Release 12.2(12k) is a rebuild release for Cisco IOS Release 12.2(12). The caveats in this section are resolved in Cisco IOS Release 12.2(12k) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms: A description of what is observed when the caveat occurs.
- Conditions: The conditions under which the caveat has been known to occur.
- Workaround: Solutions, if available, to counteract the caveat.

Basic System Services

- CSCef46191

  Symptoms: A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.

  All other device services will operate normally.

  Conditions: User initiated specially crafted TCP connection to a telnet or reverse telnet port results in blocking further telnet sessions. Whereas, services such as packet forwarding, routing protocols and all other communication to and through the device remains unaffected.

  Workaround: The detail advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml

Miscellaneous

- CSCea87364

  Symptoms: Distributed Cisco Express Forwarding (DCEF) may become disabled on a Versatile Interface Processor (VIP) or Cisco 12000 series line card (LC), and the following error message may appear on the console:

  ```
  %FIB-3-FIBDISABLE: Fatal error, slot 12: Window did not open, LC to RP IPC is non-operational
  ```

  Conditions: This symptom is observed on a Cisco 7500 series VIP2-50 and VIP4- 80 in which ATM OC-3 port adapters such as the PA-A1-OC3 or PA-A3-OC3 are installed when the Cisco 7500 series is upgraded to Cisco IOS Release 12.0(24) S or Release 12.0(24)S1. This symptom is also observed on a Cisco 12000 series LC during significant, prolonged routing table churn.

Workaround: Reload CEF on the VIP or LC by entering the **clear cef linecard** *slot-number* EXEC command.

Alternate Workaround: Restart the VIP by performing an online insertion and removal (OIR). Restart the LC by executing the **hw-module slot** *slot #* **reload** command.

- CSCee22810

  Symptoms: On a Cisco 7500 series, all PVCs may suddenly enter the down state and remain in this state for about two minutes before they come back up. During the DLCI down state, the subinterface does not go down and no notifications are observed in the message log.

  Conditions: This symptom is observed on a Cisco 7500 series that is configured with an RPS4+ or an RSP8 and that runs the rsp-jsv-mz image of Cisco IOS Release 12.2(12i). In addition, the router is configured with an 8-port serial port adapter and an HSSI port adapter, is configured for Frame Relay, and has more than 450 PVCs/DLCIs. Note that the symptom may be platform-independent and may also occur on other Cisco platforms in a similar configuration.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(12j)

Cisco IOS Release 12.2(12j) is a rebuild release for Cisco IOS Release 12.2(12). The caveats in this section are resolved in Cisco IOS Release 12.2(12j) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms: A description of what is observed when the caveat occurs.
- Conditions: The conditions under which the caveat has been known to occur.
- Workaround: Solutions, if available, to counteract the caveat.

Interfaces and Bridging

- CSCeb59227

  Symptoms: The ifOutUcastPkts, ifOutOctets, and ifHCOutOctets Simple Network Management Protocol (SNMP) counters of a Fast Ethernet subinterface may not be incremented.

  Conditions: This symptom is observed on a Cisco 7500 series when traffic is received from a serial interface in a Multiprotocol Label Switching (MPLS) network and when the Fast Ethernet subinterface is configured for dot1q encapsulation.

  Workaround: There is no workaround.

- CSCec87736

  Symptoms: TX Simple Network Management Protocol (SNMP) counters do not update on Fast Ethernet subinterfaces for distributed Cisco Express Forwarding (dCEF) traffic.

  Conditions: This symptom is observed on Cisco IOS Release 12.0(26)S and Release 12.3. The hardware is DEC21140A, and the interface receiving the traffic is not located on the same Versatile Interface Processor (VIP).

  Workaround: There is no workaround.

IP Routing Protocols

- CSCeb17467

  Symptoms: A Cisco router may reload when Border Gateway Protocol (BGP) is configured to carry Virtual Private Network version 4 (VPNv4) routes.

  Conditions: This symptom is observed when VPNv4 import processing occurs simultaneously with a BGP neighbor reset, for example, when a VPN routing and forwarding (VRF) instance is configured and you enter the **clear ip bgp *** privileged EXEC command.

  Workaround: There is no workaround.

Miscellaneous

- CSCdx77088

  Symptoms: A Cisco router may reload because of a watchdog timeout in the pool process.

  Conditions: This symptom is platform independent.

  Workaround: There is no workaround.

- CSCdz84583

  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, the attack vector does not directly compromise data integrity or confidentiality.

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

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml, and it describes this vulnerability as it applies to Cisco products that do not run Cisco IOSÆ software.

  A companion advisory that describes this vulnerability for products that run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml.

- CSCed35253

  Symptoms: A router may reload unexpectedly after it attempts to access a low memory address.

  Conditions: This symptom is observed after ACLs have been updated dynamically or after the router has responded dynamically to an IDS signature.

  Workaround: Disable IP Inspect and IDS.

- CSCed76109

  Symptoms: On a Cisco 7500 series that is equipped with Versatile Interface Processors (VIPs) with ATM port adapters, the ATM PVCs may not come back up after the ATM interface flaps. This occurs because the interfaces in the VIP do not transmit any packets but still process incoming traffic.

Conditions: This symptom is observed in a dLFIoATM environment in which distributed Class Based Weighted Fair Queueing (dCBWFQ) is configured on PPPoATM virtual templates.

Workaround: Apply any kind of distributed queueing on any interface or subinterface of the affected VIP. Doing so triggers all interfaces to start transmitting again, enabling the ATM PVCs to come back up.

- CSCed93836

  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 IOSÆ 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.

- CSCee06794

  Symptoms: DTS may not work properly on dot1q Fast Ethernet subinterfaces. Traffic is not shaped at the expected rate

  Conditions: This problem is observed on a Cisco 7500 series router that is configured as a PE router and that runs Cisco IOS Release 12.2(12i). The symptom may also occur in other releases.

  Workaround: If this is an option, use ISL subinterfaces.

- CSCee41842

  Symptoms: “%TAGCON-3-LCLTAG_ALLOC: Cannot allocate local tag” error messages are seen in the log as MPLS labels are not being freed properly.

  Conditions: This label leak problem has been noticed in BGP VPN when a locally learned VPN prefix becomes a remote prefix. This will happen if a set of routes has at least one local path via CE (could be EBGP learned or redistributed from VRF IGP) and one IBGP learned remote path. If the local CE learned path flaps for some reason, there is a possible label leak caused by BGP.

  Workaround: Increase the label range using the **mpls label range x y** command.

Resolved Caveats—Cisco IOS Release 12.2(12i)

Cisco IOS Release 12.2(12i) is a rebuild release for Cisco IOS Release 12.2(12). The caveats in this section are resolved in Cisco IOS Release 12.2(12i) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms: A description of what is observed when the caveat occurs.

- Conditions: The conditions under which the caveat has been known to occur.
- Workaround: Solutions, if available, to counteract the caveat.

Basic System Services

- CSCed44414

  Symptoms: When the slave RSP crashes, a QAERROR is observed in the master console, resulting in a cbus complex. The cbus complex will reload all the VIPs in the router.

  Conditions: This symptom happens when the slave crashes in a period when there is a large number of packets going towards the RSP. A large number of packets go to the RSP when CEF switching is configured or when routing protocol updates are numerous.

  Workaround: There is no workaround.

Miscellaneous

- CSCed45746

  Symptoms: Several prefixes for non-redistributed connected interfaces in different VRFs may be partially bound to the same MPLS-VPN label, thus disrupting traffic bound to one or more of these VRFs.

  Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2(6f)M1 and Release 12.2(12f). The symptom appears after flapping on the VRF interfaces.

  Workaround: Clear the routes in the VRFs in sequence.

- 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.

- CSCed68575

  Cisco Internetwork Operating System (IOS) Software releases trains 12.0S, 12.1E, 12.2, 12.2S, 12.3, 12.3B and 12.3T may contain a vulnerability in processing SNMP requests which, if exploited, could cause the device to reload.

  The vulnerability is only present in certain IOS releases on Cisco routers and switches. This behavior was introduced via a code change and is resolved with CSCed68575.

  This vulnerability can be remotely triggered. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS).

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-snmp.shtml

Wide-Area Networking

- CSCec83030

  Symptoms: A parity error on a Versatile Interface Processor (VIP) card may cause other VIPs to go to a wedged state.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(12h)

Cisco IOS Release 12.2(12h) is a rebuild release for Cisco IOS Release 12.2(12). The caveats in this section are resolved in Cisco IOS Release 12.2(12h) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms: A description of what is observed when the caveat occurs.
- Conditions: The conditions under which the caveat has been known to occur.

- Workaround: Solutions, if available, to counteract the caveat.

Basic System Services

- CSCdv46906

  Symptoms: A router may send linkUp traps with the loclfReason attribute set as ‘Down’ and linkDown traps with the loclfReason attribute set as ‘Up.’

  Conditions: This symptom is observed on a Cisco router.

  Workaround: Query the link status using the command-line interface (CLI) or Simple Network Management Protocol (SNMP).

- CSCdy54493

  Symptoms: The following error message may be displayed during a Simple Network Management Protocol (SNMP) query on a ciscoFlashDeviceEntry:

  ```
  %SNMP-3-CPUHOG: Processing GetNext of ciscoFlashDeviceEntry.5.8
  ```

  Conditions: This symptom may occur on any Cisco platform that is running Cisco IOS software.

  Workaround: Exclude ciscoFlashMIB by entering the **snmp-server** global configuration command. If SNMP must be enabled on the Flash devices, there is no workaround; however, this error message indicates only a temporary CPU high load condition, which typically does not impact router operations.

Interfaces and Bridging

- CSCdy47536

  Symptoms: A Route Switch Processor (RSP) on a router may reload when a subinterface of a 1-port Fast Ethernet 100BASE-TX port adapter (PA-FE-TX) that is configured with dot1q encapsulation is removed.

  Conditions: This symptom is observed on the RSP of a Cisco router that is running Cisco IOS Release 12.2(12.5). The RSP card has a PA-FE-TX port adapter with a subinterface that is configured with dot1q encapsulation.

  Workaround: Shut down and remove the subinterface that is configured with dot1q encapsulation.

- CSCin11537

  Symptoms: An ATM interface may not come up after the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command is entered.

  Conditions: This symptom is observed on a Catalyst 5000 Route Switch Module (RSM) that is running Cisco IOS Release 12.2(10).

  Workaround: There is no workaround.

- CSCin14406

  Symptoms: A Packet-over-SONET double-wide single-mode port adapter (PA-POSdw-SM) is not recognized on a Cisco router.

  Conditions: This symptom is observed on a Cisco 7500 series.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCea43167

  Symptoms: In a large Border Gateway Protocol (BGP) Open Shortest Path First (OSPF) environment, the OSPF neighbors may go down when the BGP link flaps and a large number of BGP routes are flushed out of the route table or are repopulated.

  Conditions: The conditions under which this symptom occurs seem to depend upon when the BGP configuration is applied to the router. There is no OSPF neighbor drop if the router reloads without the BGP configuration and BGP is added after the router reloads. However, the router drops OSPF neighbors when a BGP link flaps if BGP is already configured before the router is reloaded.

  Workaround: There is no workaround.

- CSCeb85136

  Symptoms: An IP packet that is sent with an invalid IP checksum may not be dropped.

  Conditions: This symptom is observed if the IP checksum is calculated with a decreased time-to-live (TTL) value. For example, in the situation where the IP checksum must be 0x1134 with a TTL of 3, if the packet is sent with an IP checksum of 0x1234 that is calculated by using a TTL value of 2, the packet is not dropped. In all other cases, packets with incorrect checksums are dropped.

  Workaround: There is no workaround.

Miscellaneous

- CSCdv01994

  Symptoms: Memory allocation failures (MALLOCFAIL) may be observed on a router after it is reloaded.

  Conditions: This symptom is observed on a Cisco 7500 series router.

  Workaround: There is no workaround.

- CSCdx65248

  Symptoms: Cisco Express Forwarding (CEF) may be disabled on a line card after a memory leak occurs.

  Conditions: This symptom is observed on a line card.

  Workaround: There is no workaround.

- CSCdy17399

  Symptoms: Internal Border Gateway Protocol (iBGP) load balancing does not function correctly on a Route Processor Module (RPM-PR) line card.

  Conditions: This symptom is observed when the iBGP unequal-cost multipath load-balancing feature is enabled on a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN).

  Workaround: There is no workaround.

- CSCea84387

  Symptoms: A user session may pause indefinitely, causing a Cisco router to become unresponsive.

  Conditions: This symptom is observed when multiple simultaneous users enter modular QoS CLI (MQC) commands on the same router via separate vty sessions.

  Workaround: Allow only one user at a time to enter MQC commands.

- CSCeb73681

  Symptoms: The main High-Speed Serial Interface (HSSI) interface flaps when you enter the **map-class frame-relay** global configuration command on a subinterface.

  Conditions: This symptom is observed only when map class contains both traffic shaping and Random Early Detection (RED).

  Workaround: Use only traffic shaping under the map-class.

- CSCec15517

  Symptoms: A router may reload when the **show policy-map interface** EXEC command is issued.

  Conditions: It is unclear at this time what conditions must exist to trigger this symptom. A preliminary review indicates that the problem may exist in the **show policy-map interface** code when a Frame Relay (FR) permanent virtual circuit (PVC) policy is shown.

  Workaround: There is no workaround.

- CSCec38322

  Symptoms: A Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) provider edge (PE) router that is running distributed Cisco Express Forwarding (dCEF) may have high memory usage and memory allocation failures when dCEF is disabled and then reenabled.

  Conditions: This symptom is observed on a PE router that has a large number of VPN routes (over 30,000) in a VPN routing/forwarding (VRF) table when CEF is disabled and then reenabled.

  Further Problem Description: View the output of the **show processes memory** EXEC command to verify that the CEF process memory usage increases.

  Workaround: Reload the router.

- CSCin41510

  Symptoms: An output service policy with a police feature may be rejected, and the following error message may be generated:

  ```
  Cannot attach flat policy to pvc/sub-interface. Hierarchical policy with shape in
  class-default is recommended
  ```

  Conditions: This symptom is observed when the output service policy is attached to multiple subinterfaces.

  Workaround: There is no workaround.

- CSCuk39189

  Symptoms: Leaks may be observed for some Virtual Private Network routing and forwarding (VRF) routes in the global Forwarding Information Base (FIB) table when a VRF is deleted and recreated.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.0 S or Release 12.2 T.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCdy16633

  Symptoms: A Cisco router may reload during the Multilink PPP (MLP) process.

  Conditions: This symptom is observed when the MLP is trying to bundle ISDN dial-up connections. The reload occurs when interfaces that belong to the bundle are brought up and down.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(12g)

Cisco IOS Release 12.2(12g) is a rebuild release for Cisco IOS Release 12.2(12). The caveats in this section are resolved in Cisco IOS Release 12.2(12g) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms: A description of what is observed when the caveat occurs.
- Conditions: The conditions under which the caveat has been known to occur.
- Workaround: Solutions, if available, to counteract the caveat.
- CSCdz15937

  Symptoms: Border Gateway Protocol (BGP) may install Tag Forwarding Information Base-Virtual Private Network version 4 (TFIB-VPNv4) entries for some prefixes without any change in the incoming or outgoing tags for the prefix.

  Conditions: This symptom is observed on an Autonomous System Boundary Router (ASBR) that is performing VPNv4 label exchange.

  Workaround: There is no workaround.
- CSCea12346

  Symptoms: The **show policy interface** EXEC command may display incorrect bandwidth allocation among child classes if the class is configured with the **bandwidth percent** policy-map class configuration command or the **priority percent** policy-map class configuration command.

  Conditions: This symptom is observed when a hierarchical service policy is applied to a Frame Relay map class.

  Workaround: There is no workaround.
- CSCea74631

  Symptoms: A Route Switch Processor (RSP) that is acting as a slave may have complete packet switching activity interrupted for several minutes. This situation may cause the RSP to permanently pause.

  Conditions: This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2(12d).

  Workaround: There is no workaround.
- CSCea84736

  Symptoms: After you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface, pings may fail on this interface.

  Conditions: This symptom is observed on an interface that has both PPP and Intermediate System-to-Intermediate System (IS-IS) configured.

  Workaround: There is no workaround.
- CSCeb68061

  Symptoms: In an interautonomous setup in the Autonomous System Boundary Router (ASBR), the label for a prefix in the label forwarding information base (LFIB) may be inconsistent with the actual label in the multiprotocol external Border Gateway Protocol (MP-eBGP) table.

  Conditions: This symptom is observed on Cisco routers that are running CiscoIOS Release12.2.

Workaround: Execute the **clear ip bgp** *neighbor-address* privileged EXEC command where *neighbor-address* is the address of the eBGP peer from which we learn the route to the prefix whose label is wrong.

Resolved Caveats—Cisco IOS Release 12.2(12f)

Cisco IOS Release 12.2(12f) is a rebuild release for Cisco IOS Release 12.2(12). The caveats in this section are resolved in Cisco IOS Release 12.2(12f) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms: A description of what is observed when the caveat occurs.
- Conditions: The conditions under which the caveat has been known to occur.
- Workaround: Solutions, if available, to counteract the caveat.
- CSCdy79465

  Symptoms: A VPN routing/forwarding (VRF) static route pointing to Null0 may not have an aggregate label. Redistribution into the VRF (redistribute static) may cause packets to be dropped.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(13).

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(12e)

Cisco IOS Release 12.2(12e) is a rebuild release for Cisco IOS Release 12.2(12). The caveats in this section are resolved in Cisco IOS Release 12.2(12e) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

- Symptoms: A description of what is observed when the caveat occurs.
- Conditions: The conditions under which the caveat has been known to occur.
- Workaround: Solutions, if available, to counteract the caveat.
- 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.

- CSCdz32940

  Symptoms: A Cisco router may reload unexpectedly when saving the configuration to NVRAM.

  Conditions: This symptom is observed on a Cisco router that is configured with the **service compress-config** global configuration command.

  Workaround: Enter the **no service compress-config** global configuration command.

  Alternate workaround: Use the **boot config filename nvbypass** global configuration command.

- CSCdz71127

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

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

  This advisory is available at

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

- CSCea02355

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

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

  This advisory is available at

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

- 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.

- CSCea72272

  Symptoms: The startup configuration file may become corrupt.

  Conditions: This symptom is observed when there are multiple Telnet sessions simultaneously executing the **copy running-config startup-config** command.

  Workaround: Reissue the **copy running-config startup-config** command to save the configuration correctly. The operation should be done by only one Telnet session.

Resolved Caveats—Cisco IOS Release 12.2(12c)

Cisco IOS Release 12.2(12c) is a rebuild release for Cisco IOS Release 12.2(12). The caveats in this section are resolved in Cisco IOS Release 12.2(12c) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

Symptoms: A description of what is observed when the caveat occurs.

Conditions: The conditions under which the caveat has been known to occur.

Workaround: Solutions, if available, to counteract the caveat.

- CSCdx39499

  Symptoms: A port adapter may stop receiving packets. When this symptom occurs, the output of the **show interface** EXEC command does not report any input or output drops. When the **show controller** EXEC command is issued on the Versatile Interface Processor (VIP) console of a router, the command output may display incrementing rx_no_buffer and virtual circuit connection (VCC) counts.

  Conditions: These symptoms are observed on the enhanced ATM Port Adapter (PA-A3) of a Cisco 7500 series router.

  Workaround: Bounce the port adapter interface by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCdy53391

  Symptoms: The **show interface** input and output rate counters will show zero for a tunnel interface.

  Conditions: This symptom will occur only on the Cisco 7500 series routers.

  Workaround: There is no workaround.

- CSCdy62338

  Symptoms: The **show bootflash: chips** EXEC command may cause subsequent commands such as the **show bootflash all** EXEC command to fail.

  Conditions: This symptom is observed on a Cisco router that has a Route Switch Processor 8 (RSP8) and that is running Cisco IOS Release 12.2(6d) or Release 12.2(6f). This symptom occurred because the bootflash module was flawed.

  Workaround: Enter the **show version** EXEC command to restore the router to normal operating condition or reseat/replace the flash SIMM.

Resolved Caveats—Cisco IOS Release 12.2(12b)

Cisco IOS Release 12.2(12b) is a rebuild release for Cisco IOS Release 12.2(12). The caveats in this section are resolved in Cisco IOS Release 12.2(12b) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

Symptoms—A description of what is observed when the caveat occurs.

Conditions—The conditions under which the caveat has been known to occur.

Workaround—Solutions, if available, to counteract the caveat.

- CSCdu45300

  Symptoms After the parameters of a virtual circuit (VC) are modified, a 500-ms delay may be observed on the VC when it is updated. This behavior may cause the router to appear to pause indefinitely when a modified VC class is applied to the VC.

  Conditions This symptom is observed on a Cisco router when the parameters of a VC are modified.

  There are other defects associated with CSCdu45300 that have been ported to Cisco IOS Release 12.2. Together with CSCdu45300, the following DDTS entries have also been committed to address such defects:

  – CSCin08167

  - CSCdv67275
  - CSCdv71213

  Workaround There is no workaround.

- CSCdv55152

  Symptoms When an existing virtual circuit (VC) class is modified or removed or when a new VC class is attached, the router may appear to pause indefinitely. Data packets may be lost when this symptom occurs.

  Conditions This symptom is observed on a Cisco 7200 series that is running Cisco IOS Release 12.2(5).

  There are other defects associated with CSCdu45300 that have been ported to Cisco IOS Release 12.2. Together with CSCdu45300, the following DDTS entries have also been committed to address such defects:

  - CSCin08167
  - CSCdv67275
  - CSCdv71213

  Workaround There is no workaround.

- CSCdv67275

  Symptoms A virtual circuit (VC) may fail after permanent virtual circuit (PVC) parameters are modified. When this symptom occurs, unexpected behavior may also be observed with existing PPP sessions on the PVC.

  Conditions This symptom is observed on a Cisco 7200 series that is running Cisco IOS Release 12.2 T.

  Workaround There is no workaround.

- CSCdv71213

  Symptoms A Cisco Route Switch Processor (RSP) router may reload after a configured ATM permanent virtual circuit (PVC) is removed.

  Conditions This symptom is observed on a Cisco RSP router that is running Cisco IOS Release 12.2 T.

  Workaround There is no workaround.

- CSCdw41164

  Symptoms A Versatile Interface Processor (VIP) may reload because of an error at the ct3sw_check_tx process.

  Conditions This symptom is observed on a Cisco 7000 series VIP that is running Cisco IOS Release 12.0(16)S4.

  Workaround There is no workaround.

- CSCdx82485

  Symptoms Under rare circumstances, a router that is configured with Protocol-Independent Multicast (PIM) may pause indefinitely.

  Conditions This symptom is observed when an interface that has PIM enabled is shut down. This symptom may also occur when other configuration operations are performed on a PIM-enabled interface. This symptom affects only port adapters such as the 8-port 10BASE-T Ethernet port adapter (PA-8E) and the 8-port 10BASE-T Ethernet port adapter (PA-4E) that are using a particular third-party vendor chip.

Workaround Use a different Ethernet card, or avoid using PIM.

- CSCdx89548

  Symptoms An interface on a Cisco 7500 series channelized T3 port adapter cannot ping a directly connected interface because of adjacency difficulties.

  Conditions The conditions under which these symptoms occur are not known at this time.

  Workaround Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface on the channelized T3 port adapter.

- CSCdy09517

  Symptoms Voice packets may assume the source address of a serial subinterface even after the **h323-gateway voip bind srcaddr** *ip_address* interface configuration command is configured on a different interface. This symptom is observed on the first call or the first set of calls after the router is reloaded. The second and subsequent calls work normally and have voice packets that have the correct source address.

  Conditions This symptom is observed on a Cisco 2600 series or Cisco 3600 series that is running Voice over IP (VoIP) over Frame Relay and quality of service (QoS).

  Workaround Add a line to the VoIP access control list (ACL) to permit voice packets that have User Datagram Protocol (UDP) ports in the range of 16384 to 32767 and use the source address of the serial subinterface.

- CSCdy24774

  Symptoms A router may reload with a bus error or may log a CPUHOG when an ATM virtual circuit (VC) class is modified.

  Conditions This symptom is observed on a Cisco 7500 series router that has an enhanced ATM port adapter (PA-A3) and that is running Cisco IOS Release 12.2(6d).

  Workaround There is no workaround.

- CSCdy29329

  Symptoms The cache error recover function (CERF) is disabled after a Cisco 7200 series router is reloaded. This symptom is observed after CERF is enabled, written into the startup configuration, and the router is reloaded.

  The output of the **show memory cache error-recovery** EXEC command may indicate that the commands are disabled after the router is reloaded:

  ```
  no memory cache error-recovery L3 data
  no memory cache error-recovery options nvram-report
  no memory cache error-recovery options parity-check
  memory cache error-recovery options window 0
  memory cache error-recovery options max-recoveries 0
  ```

  Conditions This symptom is observed on a Cisco 7200 series router that is using a Network Processing Engine (NPE-300) that has 32 MB of memory in the dual in-line memory module (DIMM2).

  Workaround Install 64 MB of memory in the DIMM2.

- CSCdy33187

  Symptoms Fragmentation may not work normally for multicast traffic. An incorrect header may be used when the router runs an application that replicates and retransmits a packet.

  Conditions This symptom is observed on a Cisco 7200 series router.

  Workaround There is no workaround.

- CSCdy38335

  Symptoms A router that is configured with a 2-port Fast Ethernet 100BASE-FX port adapter (PA-2FE-TX) may reload when the packet cleanup is not performed properly in the interrupt path of the port adapter.

  Conditions This symptom is observed on a Cisco 7200 series router and a Cisco 7500 series router.

  Workaround There is no workaround.

- CSCdy41507

  Symptoms A recursive route may cause a router to reload while the router is attempting to establish the neighborhood.

  Conditions This symptom is observed when recursive routes are present on a Cisco router that is configured with Enhanced Interior Gateway Routing Protocol (EIGRP) tunnels. Recursive routes may be present because of a normal configuration or as a temporary effect that occurs when routes are cleared.

  Workaround If this symptom occurs because of the presence of a permanent recursive route, alter the configuration to remove the recursive route. If the symptom occurs when routes are cleared, there is no workaround. However, you may try to change the order in which the routes are cleared.

- CSCdy48848

  Symptoms A Versatile Interface Processor (VIP) may reload when Compressed Real-Time Protocol (cRTP) header compression is disabled on a Frame Relay interface.

  Conditions This symptom is observed on the serial interface of a Cisco router when the **no frame-relay ip tcp header-compression** interface configuration command or the **no frame-relay ip rtp header-compression** interface configuration command is entered.

  Workaround Ensure that the serial interface is shut down before cRTP header compression is disabled.

- CSCdy51437

  Symptoms A Versatile Interface Processor (VIP) may reload because of a direct memory access (DMA) receive error and may display a message that is similar to the following:

  ```
  CYASIC Error Interrupt register 0x2000000
      DMA Receive Error
  CYASIC Other Interrupt register 0x180
      QE HIGH Priority Interrupt
      Unknown CYA oisr bit 0x00000080
      QE RX HIGH Priority Interrupt
      QE TX HIGH Priority Interrupt
  CYBUS Error Cmd/Addr 0x8000068, CYBUS Error Data 0x0
  MPUIntfc/PacketBus Error register 0x0
  ```

  Conditions This symptom is observed while there is a large amount of Internet MIX (IMIX) traffic on a 2-port Fast Ethernet port adapter (PA-2FE) that is installed on the VIP of a Cisco 7500 series.

  Workaround There is no workaround.

- CSCdy57048

  Symptoms A Telnet session from a terminal over a vty connection to a Cisco 7206VXR router may pause indefinitely.

Conditions This symptom is observed on a Cisco 7206VXR router that is running Cisco IOS Release 12.2(4)XZ5, that is configured with a Network Processing Engine 300 (NPE-300), and that is functioning as a Multiprotocol Label Switching Virtual Private Network (MPLS VPN) provider edge (PE) router when large text displays are dumped on the screen of the terminal.

The symptom is caused by a corrupt TCP Telnet packet that is generated by the router.

Workaround There is no workaround.

- CSCdy76759

  Symptoms A 2-port Fast Ethernet port adapter (PA-2FE) may stop sending packets.

  Conditions This symptom is observed only when there is a heavy traffic load on the PA-2FE port adapter of a Cisco router.

  Workaround There is no workaround.

- CSCdy89255

  Symptoms An input (flat) service policy can be applied only to a single Frame Relay subinterface. The following error message may be displayed when the same input (flat) service policy is applied to a second Frame Relay subinterface:

  ```
  A flat policy can be attached to only one sub-interface/pvc. Remove the flat policy
  and retry this command
  ```

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(12).

  Workaround There is no workaround.

- CSCdz05759

  Symptoms A user configuration may be rejected.

  Conditions This symptom is observed when a router is loaded with an older image that supports the configuration of police action through the use of numerics (0 through 64) rather than through the use of alphanumerics.

  The user configuration is rejected when the following police action commands are configured in the following configuration using alphanumerics:

  ```
  policy-map test
   class class-default
    police cir 8000
     conform-action set-dscp-transmit af11
  ```

  Workaround Reconfigure the **police conform-action set-dscp-transmit** *dscp-value* policy map configuration command using numerics.

- CSCdz09265

  Symptoms A Cisco Versatile Interface Processor 2 Model 40 (VIP2-40) may reload when a fragmentation configuration is removed.

  Conditions This symptom is observed on a Cisco 7500 series that has a VIP2-40 interface that is running Cisco IOS Release 12.2(10b) and that is running Frame Relay and fragmentation.

  Workaround Shut down the VIP2-40 interface before removing the fragmentation configuration.

- CSCdz25339

  Symptoms An unusually formatted Multicast Source Discovery Protocol (MSDP) packet may cause a memory corruption to occur and a router to reload.

  Conditions This symptom is observed on a Cisco router that has a peer relationship with a vendor router.

Workaround If this symptom is observed on a Cisco router that has a peer relationship with vendor router, enter the **ip msdp shutdown** *peer-address* global configuration command to shut down the peer relationship with the vendor router.

- CSCdz31314

  Symptoms A 2-port Fast Ethernet port adapter (PA-2FE) that is used on a Cisco 7200 series router or on the Versatile Interface Processor (VIP) of a Cisco 7500 series router may become stuck. This symptom may also be observed on a Fast Ethernet interface that is used on the Cisco 7200 series 2-port 10/100 auto-sensing Fast Ethernet input/output controller (C7200-I/O-2FE/E).

  When the PA-2FE port adapter is used on the VIP of a Cisco 7500 series router, the VIP may reload unexpectedly and display the following output when the **show controllers vip** *slot-number* **logging** EXEC command is entered:

```
00:34:32: RX FIFO was stuck - forced to reset MAC
00:34:34: RX FIFO was stuck - forced to reset MAC
00:34:37: RX FIFO was stuck - forced to reset MAC
00:34:43: %VIP-3-MVIP_CYBUSERROR_INTERRUPT: A Cybus Error occurred.
00:34:44:
CYASIC Error Interrupt register 0x2000000 DMA Receive Error
CYASIC Other Interrupt register 0x0
CYBUS Error Cmd/Addr 0x763AD80, CYBUS Error Data 0x0
MPUIntfc/PacketBus Error register 0x0
```

  When these symptoms occur, “RX FIFO was stuck - forced to reset MAC” log messages may be observed on a Cisco 7200 series router and in the log messages on the VIP of a Cisco 7500 series router.

  Conditions These symptoms are observed when Inter-Switch Link (ISL) and Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) are used on a PA-2FE port adapter or when a Fast Ethernet interface is used on the C7200-I/O-2FE/E controller when there is a high traffic rate.

  Workaround There is no workaround.

- CSCdz53326

  Symptoms B channels may pause indefinitely in the “S_TSP_WAIT_RELEASE” state.

  Conditions This symptom is observed on the B channels of a Cisco router that is running Cisco IOS Release 12.2(6c).

  Workaround There is no workaround.

- CSCdz60229

  Cisco devices which run IOS and contain support for the Secure Shell (SSH) server are vulnerable to a Denial of Service (DoS) if the SSH server is enabled on the device. A malformed SSH packet directed at the affected device can cause a reload of the device. No authentication is necessary for the packet to be received by the affected device. The SSH server in Cisco IOS is disabled by default.

  Cisco will be making free software available to correct the problem as soon as possible.

  The malformed packets can be generated using the SSHredder test suite from Rapid7, Inc. Workarounds are available. The Cisco PSIRT is not aware of any malicious exploitation of this vulnerability.

  This advisory is available at:
  http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml

- CSCdz64355

  Symptoms A router may reload.

Conditions This symptom is observed on a Cisco 7500 series router that has a Versatile Interface Processor (VIP) after the router is upgraded to Cisco IOS Release 12.2(12b). This symptom is observed if an ATM interface state changes while one or more permanent virtual circuits (PVCs) has the **random-detect** interface configuration command enabled.

Workaround Configure the **random-detect** interface configuration command under the modular quality of service (QoS) command-line interface (CLI).

- CSCin08167

  Symptoms A virtual circuit may enter the INACTIVE state after the quality of service (QoS) parameters of the virtual circuit are modified.

  Conditions This symptom is observed when the QoS parameters of the virtual circuit are changed from "VBR" to "CBR/ABR." After the change is made, the creation of the virtual circuit fails and the virtual circuit will enter the INACTIVE state.

  Workaround Delete and recreate the virtual circuit if the QoS parameters of the virtual circuit must be modified.

- CSCin24544

  Symptoms A permanent virtual connection (PVC) configuration is removed if a PVC fails when it is recreated.

  Conditions This symptom is observed on a Cisco 7500 series that has a Versatile Interface Processor (VIP). The PVC configuration may be removed if the VIP is carrying data traffic and the parameters of the virtual circuit (VC) class that is attached to the configured PVCs on the associated interface are modified.

  Workaround There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(12a)

Cisco IOS Release 12.2(12a) is a rebuild release for Cisco IOS Release 12.2(12). The caveats in this section are resolved in Cisco IOS Release 12.2(12a) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

Symptoms—A description of what is observed when the caveat occurs.

Conditions—The conditions under which the caveat has been known to occur.

Workaround—Solutions, if available, to counteract the caveat.

- CSCdy03204

  Symptoms An Ethernet driver on an Ethernet interface may receive and forward packets that are not destined for itself.

  Conditions This symptom is observed on an Ethernet interface that has the promiscuous mode enabled in a network that has multiple Hot Standby Router Protocol (HSRP) groups. This symptom is also observed when no transparent bridging is occurring.

  Workaround There is no workaround.

- CSCdy20170

  Symptoms Poor fax and voice quality may be observed on a Cisco 7200VXR router that has an enhanced digital voice port adapter (PA-VXC+) or a multiservice interchange (MIX)-enabled port adapter (PA-MCX). This symptom occurs because of clock synchronization issues with the remote PBX or public switched telephone network (PSTN).

  This symptom can be corrected by entering the **frame-clock-select** command to configure the primary clock on the Cisco 7200VXR to avoid frame slips that occur when a clock is unsynchronized.

  Conditions This symptom is observed on a Cisco 7200VXR router that has a PA-VXC+ or PA-MCX port adapter.

  Workaround This symptom can be corrected by entering the **frame-clock-select** command to configure the primary clock on the Cisco 7200VXR to avoid frame slips that occur when a clock is unsynchronized.

- CSCdy26606

  Symptoms A Versatile Interface Processor (VIP) that has a High-Speed Serial Interface (HSSI) reloads continuously after the router is reloaded.

  Conditions This symptom is observed when the HSSI interface is in the shutdown state and when it is configured for Frame Relay encapsulation while a quality of service (QoS) with priority feature is enabled.

  Workaround Enter the **no shutdown** interface configuration command on the interface or remove the QoS policy before reloading the router.

- CSCdy40192

  Symptoms One-way audio may be observed and packets may be dropped on the serial interface of the outgoing data-link connection identifier (DLCI) on a Cisco 7507 router. The data connectivity slows and eventually stops, after which, no packets are received on the remote router.

  Conditions This symptom is observed on a Cisco 7507 router that has a Versatile Interface Processor (VIP) that is configured for Voice over Frame Relay (VoFR) using the VIP-based Frame Relay Forum implementation agreement for VoFR (FRF.11) and the Frame Relay Forum implementation agreement for VoFR (FRF.12). The Cisco 7507 router is set up for VoFR calls to a remote Cisco 2600

series router that has calls that terminate on an analog phone on a Foreign Exchange Station (FXS) port. The user on the Cisco 7507 can hear the user on the Cisco 2600, but the user on the Cisco 2600 cannot hear anything.

Workaround There is no workaround.

- CSCdy51658

  Symptoms Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) updates are not received on a single-port Fast Ethernet 100BASE-TX port adapter (PA-FE-TX) of a Cisco 7200 series. The PA-FE-TX port adapter does not receive the OSPF, EIGRP, and RIP updates on the Cisco 7200 series because multicast entries are not added in the hardware address filter.

  Conditions This symptom is observed on a PA-FE-TX port adapter of a Cisco 7200 series.

  Workaround There is no workaround.

- CSCdy52947

  Symptoms A Cisco router that is running the Cisco General Packet Radio Service (GPRS) support node (GGSN) release 1.4 image of Cisco IOS Release 12.2(10a) may reload if a create Packet Data Protocol (PDP) request message is received on an existing PDP context that has a new recovery information element (IE).

  Conditions The Cisco router reloads if the new create request that is received has the same target identifier (TID) but a different recovery IE. This symptom is observed after a PDP context is successfully opened while charging is disabled on the Cisco router.

  Workaround There is no workaround.

- CSCdy53351

  Symptoms A Cisco router that is running Cisco General Packet Radio Service (GPRS) support node (GGSN) release 1.4 software may leak memory if a new create or delete Packet Data Protocol (PDP) request message is received on an existing PDP context that is waiting for a RADIUS and Dynamic Host Configuration Protocol (DHCP) server response.

  Conditions This symptom is observed only if the create or delete PDP request is not a retry request and contains a different GPRS Tunneling Protocol (GTP) sequence number from the earlier request. This symptom is observed if the GGSN is waiting for a response from the RADIUS or DHCP server.

  Workaround There is no workaround.

- CSCdy61222

  Symptoms A Cisco router that is running Cisco General Packet Radio Service (GPRS) support node (GGSN) release 1.4 software may leak memory in the I/O buffer if either of the following conditions is present:

  – An error indication message is received on an existing Packet Data Protocol (PDP) context.

  – A delete request is received on a context that is waiting for a RADIUS or Dynamic Host Configuration Protocol (DHCP) server response, and GGSN does not return the delete response.

  Conditions This symptom is observed if the Cisco router that is running serving GPRS support nodes (SGSNs) reboots and loses all PDP contexts, and GGSN continues to send packets on the context without detecting this condition. The delete request may occur if RADIUS or DHCP takes a longer time than expected to respond to the GGSN.

  Workaround There is no workaround.

- CSCin16706

  Symptoms Open Shortest Path First (OSPF) multicast packets are not received on a 1-port Fast Ethernet 100BASE-TX port adapter (PA-FE-TX).

  Conditions This symptom is observed on a PA-FE-TX port adapter on a Cisco 7500 router that is configured with OSPF. The PA-FE-TX does not receive OSPF multicast traffic because MAC multicast entries are not added to the MAC table.

  Workaround There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(12)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(12). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(12). This section describes severity 1 and 2 caveats and select severity 3 caveats.

The following information is provided for each caveat:

- **Symptoms**—A description of what is observed when the caveat occurs.
- **Conditions**—The conditions under which the caveat has been known to occur.
- **Workaround**—Solutions, if available, to counteract the caveat.

Basic System Services

- CSCdt00950

  Symptom A router may reload with a bus error.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 11.2(18)P, 12.0(10), 12.0(5)XK1, 12.1(3)T, 12.1(4) or 12.2(7).

  Workaround There is no workaround.

- CSCdw50718

  Symptoms A router may reload because of a memory corruption.

  Conditions This symptom is observed when a Simple Network Management Protocol (SNMP) is set to the snmp-set smonVlanIdStatsTable elem 64-bit counter. The reload happens only when this counter is set to certain values.

  Workaround There is no workaround except to disable SNMP.

- CSCdw52694

  Symptoms You may not be able to restart or reschedule an active Response Time Reporter (RTR) probe. Attempts to do so result in the probe being shown with a status of "Unknown" when the **show rtr operation** command is executed.

  Condition This situation has been observed on Cisco 2611 routers running Cisco IOS Release 12.2(5).

  Workaround Enter the **no rtr** command and reconfigure the RTR probe. Note that the **no rtr** command will disable all of the RTR probes and must be used with utmost caution.

- CSCdw56864

  Symptoms Incorrect bearer capability is detected when a call is made using a vendor-specific program to a router.

  Conditions This symptom is observed on a Cisco 3810 router that is running Cisco IOS Release 12.2(6).

  Workaround There is no workaround.

- CSCdw52694

  Symptoms You may not be able to restart or reschedule an active Response Time Reporter (RTR) probe. Attempts to do so result in the probe being shown with a status of "Unknown" when the **show rtr operation** command is executed.

  Condition This situation has been observed on Cisco 2611 routers running Cisco IOS Release 12.2(5).

  Workaround Enter the **no rtr** command and reconfigure the RTR probe. Note that the **no rtr** command will disable all of the RTR probes and must be used with utmost caution.

- CSCdw85004

  Symptoms The Response Time Reporter (RTR) uses random User Datagram Protocol (UDP) ports to respond to Service Assurance Agent (SAA) probes.

  Conditions This symptom is observed on a Cisco router.

  Workaround There is no workaround.

- CSCdx15180

  Symptoms The **snmp-server host** global configuration command may not be accepted on a router. The **snmp-server host** global configuration command may also disappear from the configuration after the router is reloaded.

  Conditions This symptom is observed on a Cisco 2600 router that is running Cisco IOS Release 12.2(6) or Release 12.2(7).

  Workaround There is no workaround.

- CSCdx20135

  Symptoms A router may display a "%RADIUS-3-ALLDEADSERVER" error message on the console.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2 T even if the **radius-server deadtime** global configuration command is not configured.

  Workaround There is no workaround.

- CSCdx25238

  Symptoms A channel-associated signaling (CAS) T1 call may report a high presession time in RADIUS attribute 198.

  Conditions This symptom is observed on a Cisco AS5400 universal access server that is running Cisco IOS Release 12.1(05)XM08.

  Workaround There is no workaround.

- CSCdx31828

  Symptoms An ISDN interface may remain in the "ESTABLISH_AWAITING_TEI" state.

Conditions This symptom is observed on a Cisco 1604 router that has a BRI (U) interface. The BRI U interface will not come up nor will it pass any traffic.

Workaround There is no workaround.

- CSCdx35920

  Symptoms Service Assurance Agent (SAA) latency measurements may show unrealistic spikes.

  Conditions This symptom is observed when Border Gateway Protocol (BGP) is running on a router.

  Workaround Use the Jitter Probe, which requires the Response Time Reporter (RTR) responder to be running on the remote Cisco router.

- CSCdx38234

  Symptoms Packets may be dropped on a Fast Ethernet port.

  Conditions This symptom is observed on a Fast Ethernet port that is installed on a Catalyst 6000 switch that is running Cisco IOS Release 12.1 and that is connected to the Internet. This symptom does not occur when NetFlow is enabled on a Gigabit Ethernet interface. In the affected setup, a Content Switching Module (CSM) that is on the Catalyst 6000 is used to perform Network Address Translation (NAT). This symptom may affect only traffic that is sent through the CSM for NAT when NetFlow is enabled.

  Workaround Disable Cisco Express Forwarding (CEF) on the interface that has the **ip route-cache flow** interface configuration command and the **ip nat outside** interface configuration command configured. Packets are not dropped when fast switching is used; therefore, fast switching may be used in place of CEF.

- CSCdx41219

  Symptoms The performance of the boot flash write operation is slower than normal.

  Conditions This symptom is observed on the boot flash of a Route Switch Processor (RSP).

  Workaround There is no workaround.

- CSCdx45241

  Symptoms Incoming calls may fail if authentication, authorization, and accounting (AAA) and virtual profiles are configured on a Cisco universal access server. AAA debug output may indicate that there is an error when the PPP network control protocols are authorized. This symptom may result in the failure to negotiate the IP Control Protocol (IPCP) or other Network Control Protocols (NCPs).

  Conditions This symptom is observed on a Cisco universal access server.

  Workaround There is no workaround.

- CSCdx54922

  Symptoms A Performance Route Processor (PRP) having Border Gateway Protocol (BGP)/Interior Gateway Protocol (IGP) with Multiprotocol Label Switching Traffic Engineering (MPLS-TE) can cause exception when trying to reload the router. This leads to another reload.

  Conditions This symptom is observed on a Cisco 12000 series Internet router that is running Cisco IOS Release 12.0(21.3)S1.

  Workaround There is no workaround.

- CSCdx58579

  Symptoms A Performance Route Processor (PRP) may reload when a previously unformatted bootflash is being formatted.

Conditions This symptom is observed on a Cisco 12000 series Internet router that is running Cisco IOS Release 12.0(21.3)S1.

Workaround There is no workaround.

- CSCdx60187

  Symptoms When a permanent virtual circuit (PVC) is configured for an average bandwidth, the actual bandwidth that is used for that PVC in the transmit direction may not be accurate.

  Conditions This symptom is observed on a Cisco MC3810 access concentrator that is running Cisco IOS Release 12.2(7b).

  Workaround There is no workaround.

- CSCdx76361

  Symptoms A router that is configured with a Route Switch Processor (RSP) drops multicast packets, which leads to a loss of connectivity.

  Conditions This symptom is observed in a bridging environment, when the router that is configured with the RSP is running the rsp-jsv-mz image of Cisco IOS Release 12.2(10.7)T1 or Release 12.2(11.2) and the subscriber trunk is configured with a multicast policy that is set to ìpermit.î

  Workaround There is no workaround.

- CSCdx93215

  Symptoms A Route Switch Processor (RSP) may display ìrsp_fs_free_memd_pakî traceback messages.

  Conditions This symptom is observed on an RSP that has a Token Ring setup.

  Workaround There is no workaround.

- CSCdx96327

  Symptoms A router may reload if the **no ip routing** interface configuration command is configured on a router that has NetFlow configured.

  Conditions This symptom is observed on a router while traffic is flowing through the router on the interface that has NetFlow configured.

  Workaround Remove NetFlow before entering the **no ip routing** interface configuration command, or stop traffic from going through the interface that has NetFlow configured before entering the **no ip routing** interface configuration command.

EXEC and Configuration Parser

- CSCdx32133

  Symptoms A router may reload with a bus error at address 0x500.

  Conditions This symptom is observed on a Cisco 7500 router that has a Route Switch Processor (RSP4) and that is running Cisco IOS Release 12.2(9.4a).

  Workaround There is no workaround.

- CSCdx67594

  Symptoms A router that is configured for ISDN services may reject the **pri-group** controller configuration command when this command is configured on the T1 or E1 controllers in the running configuration when a router is booted up. This symptom may result in the loss of custom

configurations under the ISDN serial x/y:23 or the serial x/y:15 interface. The ISDN voice port assignment under the plain old telephone service (POTS) dial peers may also be lost if the router is configured for ISDN voice.

Conditions This symptom is observed if the **isdn switch-type** global configuration command appears in the running configuration after any **pri-group** controller configuration command statements under a T1 or E1 controller. If the running configuration is saved to NVRAM and the router is reloaded, the router will reject the **pri-group** controller configuration command statements and display the "%ISDN switch-type must be set first" error message.

Workaround Enter the **copy start running** command to reconfigure the **pri-group** controller configuration command statements on the ISDN serial x/y:23 or the serial x/y:15 interfaces and any ISDN voice port assignments under any POTS dial peer.

IBM Connectivity

- CSCdv31996

  Symptoms A router may display the follow error message in the router log:

  ```
  %SYS-2-LINKED: Bad enqueue of 61EC814C in queue 6202479C -Process== "<interrupt
  level>", ipl== 4
  ```

  When the router logs the message, the router may or may not respond to the attached bisynchronous or binary synchronous communication (BSC) devices.

  Conditions This symptom is observed on a Cisco router that has a 2-port serial WAN interface card (WIC-2T).

  Workaround Use half duplex on the Block Serial Tunnel (BSTUN) interface, or try using a different serial interface card such as the 4-port synchronous/asynchronous serial network module (NM-4A/S).

- CSCdw76834

  Symptoms A small buffer leak may occur on a router.

  Conditions This symptom is observed on a Cisco router that is running data-link switching (DLSw) local conversion from Synchronous Data Link Control (SDLC) to Logical Link Control, type 2 (LLC2). This condition was seen on a router only when several multidropped SDLC controllers were configured.

  Workaround Ensure that there are no Physical Unit 2.1 (PU 2.1) devices that have an exchange identification (XID) configured but that are not installed. If a specific controller is not installed, remove the configuration for the controller from the router.

- CSCdx56545

  Symptoms A software-forced reload may occur on a router.

  Conditions This symptom is observed on a Cisco 7200 router and is specific to a configuration in which a central router that is running data-link switching plus (DLSw+) is receiving a unnumbered information frame (UI-frame) such as destination service access point (DSAP) AA or source service access point (SSAP) AA from a DLSw+ remote peer. The reload occurs under certain conditions such as when the central router is computing an internal variable incorrectly. The occurrence of this symptom is specific to a DLSw+ configuration.

  Workaround Configure the **dlsw icannotreach saps aa** global configuration command on the central DLSw+ router. This command will eliminate UI-frames on service access points (SAPs) AA from the DLSW network.

- CSCdx77489

  Symptoms When the CUR_EX (CANUREACH explorer) frame is sent from a vendor-specific router to a Cisco router, an ICR_EX (I_Can_Reach explorer) frame is returned with a ì01î in the target service access point (SAP) field and the vendor-specific router rejects the ICR_EX and the CUR_CS (can u reach circuit setup) field does not flow.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2.

  Workaround Configure the end stations in a manner that would allow the connection attempts to originate from the end station that is connected locally to the Cisco data-link switching plus (DLSw+) router.

- CSCdx86037

  Symptoms A router may reload if the **no shutdown** interface configuration command is entered on the Block Serial Tunneling (BSTUN) broadband service card (BSC) before the **bsc primary** interface configuration command or the **bsc secondary** interface configuration command is added to the configuration.

  Conditions This symptom is observed on a BSTUN BSC interface of a Cisco router.

  Workaround Enter the **bsc primary** interface configuration command or the **bsc secondary** interface configuration command before entering the **no shutdown** interface configuration command on the BSTUN BSC interface.

- CSCdy07559

  Symptoms A router may unexpectedly remove an unrelated data-link switching (DLSw) circuits on other serial interfaces.

  Conditions This symptom is observed on a router that is using DLSw with Synchronous Data Link Control (SDLC) on attached serial interface controllers.

  Workaround There is no workaround.

Interfaces and Bridging

- CSCdt30389

  Symptoms On a router, the PA-2CT1/PRI and PA-2CE1/PRI port adapters may cause packets to get delayed by 100 to 200 milliseconds.

  Conditions This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.1(5)T1. The symptom is not noticeable unless interpacket delay is monitored at the output ports or channels of these port adapters for a continuous stream of packets. Furthermore, this delay has been observed for the PRI mode of operation.

  Workaround There is no workaround.

- CSCdu78921

  Symptoms A Multilayer Switch Feature Card (MSFC) may reload.

  Conditions This symptom is observed after an upgrade from Cisco IOS Release 12.0(7)XE to Release 12.1(8a)E.

  Workaround There is no workaround.

- CSCdv44508

  Symptoms A Cisco router reloads with a bus error.

Conditions This symptom has been observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2 T and has a PA-MCX port adapter that is configured with E1 fully channelized and has alternate mark inversion (AMI) line code and CRC4 framing.

Workaround There is no workaround.

- CSCdv81601

  Symptoms A very high negative value may be displayed on the out counters.

  Conditions This symptom is observed on a Cisco 7100 router that is running Cisco IOS Release 12.1(9E). This symptom occurs if the packets from the hold queue are dropped.

  Workaround There is no workaround.

- CSCdw65799

  Symptoms An ATM permanent virtual connection (PVC) may remain in the “INAC” state after it is configured.

  Conditions This symptom is observed on a Cisco router that is running the c7200-p-mz.122-7.4.S image of Cisco IOS Release 12.2(7.4)S.

  Workaround Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM interface to restore the PVC.

- CSCdw75291

  Symptoms An autoinstall feature may not function properly.

  Conditions This symptom is observed when a Cisco 7204VXR router is autoinstalled with a T3 connection.

  Workaround There is no workaround.

- CSCdw87343

  Symptoms The following traceback messages may be displayed when Multiprotocol Label Switching (MPLS) Weighted Random Early Detection (WRED) is tested:

  ```
  %IPC-5-SLAVELOG: VIP-SLOT3: %SYS-2-INLIST: Buffer in list, ptr= 60B3C540 -Process=
  "<interrupt level>", ipl= 2, pid= 15 -Traceback= 600BA170 60165964 60166724
  %SYS-2-INLIST: Buffer in list, ptr= 60B39EC0
  ```

  Conditions This symptom occurs when MPLS WRED is tested with WRED configured to use default queue thresholds. Pings that are sent from a Pagent router to a destination fail.

  Workaround Since this is a regression, use an IOS version which does not include CSCdw38944.

- CSCdw89164

  Symptoms A memory allocation failure (MALLOCFAIL) message is displayed when a cable is unplugged from the serial interface of a router.

  Conditions This symptom is observed on a Cisco 7200 series router when a Cisco IOS release that contains the fix for CSCdt40038 is used. This symptom affects the PA-4T, PA-8T, PA-H, PA-E3, and PA-T3 port adapters. The occurrence of this symptom depends on the erroneous bit patterns that are received from the serial line that is down.

  Workaround Bring the line back up to enable the memory usage to return to normal.

- CSCdx21115

  Symptoms The controller may send frames that are learned via sequence number protection (SNAP) without SNAP encapsulation.

  Conditions This symptom is observed if forward error correction (FEC) is configured on a Cisco 7200-I/O-2FE/E Input/Output controller.

Workaround Use Inter-Switch Linking (ISL) instead of dot1q encapsulation.

Alternate Workaround A Disable fast switching.

Alternate Workaround B Use a different type of encapsulation instead of SNAP encapsulation.

- CSCdx27009

  Symptoms An IP ping does not go through on the bridging and the bridging-to-routing path.

  Conditions This symptom is observed in an integrated routing and bridging (IRB) environment. Pings can be sent through the routing and the routing-to-bridging path, but pings cannot be sent through on the bridging and the bridging-to-routing path.

  Workaround There is no workaround.

- CSCdx30042

  Symptoms A router may reload if a circuit that has compression configured is removed while there is subsequent activity on a compression retry timer.

  Conditions This symptom is observed on a Cisco router that is using software or hardware compression and that has FRF.9 Frame Relay compression configured. The activity on the compression retry timer occurs because of a transmission error and subsequent signaling of a compression restart sequence.

  Workaround There is no workaround.

- CSCdx44664

  Symptoms For Cisco IOS releases that have the fix for CSCdp46738, the two following symptoms may be observed with Frame Relay Forum 9 (FRF.9) payload compression:

  a. The router is not able to bring up compression when it is used with another router that is running a Cisco IOS release that does not have the fix for CSCdp46738.

  b. If both the “software” and the “skip-zero-sync” options are specified, the **frame-relay map** interface configuration command and the **frame-relay payload compression** interface configuration command would not be taken in the saved configuration.

  Conditions These symptoms are observed on routers that are running a Cisco IOS release that contains the fix for CSCdp46738.

  Workaround Use the following respective workarounds for each symptom:

  a. Use a Cisco IOS release that contains the fix for CSCdp46738 and CSCdv47081. The fix for CSCdv47081 addressees issues that are brought about by the fix for CSCdp46738.

  b. Reenter the **frame-relay map** interface configuration command and the **frame-relay payload compression** interface configuration command after the router reloads.

- CSCdx49370

  Symptoms When weighted fair queueing (WFQ) is configured on a serial interface, a link may start flapping.

  Conditions This symptom is observed on a Cisco 7500 series router.

  Workaround Perform a microcode reload.

- CSCdx49398

  Symptoms A router may reload if Inter-Switch Link (ISL) VLANs are configured.

  Conditions This symptom is observed on a Cisco 7500 series router when Cisco IOS Release 12.0(21.3)S is being loaded.

  Workaround There is no workaround.

- CSCdx53809

  Symptoms A router may drop Inter-Switch Link (ISL)-encapsulated packets.

  Conditions This symptom is observed on a Cisco 7500 router that has ISL subinterfaces that are not configured for distributed switching.

  Workaround Enable distributed switching on the router by entering the **ip cef distributed** global configuration command, or use 802.1Q encapsulation instead of ISL encapsulation.

- CSCdx65955

  Symptoms When the last VLAN is removed on an interface, the interface maximum transmission unit (MTU) may be set to less than the default value of 1524.

  Conditions This symptom is observed only on Fast Ethernet and Gigabit Ethernet interfaces.

  Workaround There is no workaround.

- CSCdx68871

  Symptoms A large number of alignment errors may be observed on a router. If this symptom is combined with other high CPU-usage events such as route flapping, the router may reload.

  Conditions This symptom is observed on a Cisco 7200 router that is running Cisco IOS Release 12.2(5) and that has dot1q trunking configured.

  Workaround There is no workaround.

- CSCdx83220

  Symptoms vbr3-nrt connections get converted to ubr connections after a reload.

  Conditions After upgrading to new image, Variable Bit Rate (VBR) VCs are converted to Unspecified Bit Rate (UBR) when peak cell rate (PCR) is equal to sustained cell rate (SCR) and the maximum burst size (MBS) value is given.

  Workaround If PCR is equal to SCR, do not give the MBS value.

- CSCdx87965

  Symptoms A router that is configured with a multichannel port adapter reloads because of a bus error exception.

  Conditions This symptom is observed when link flaps occur or interfaces are reset on a router that is configured with PA-MC-T1, PA-MC-E1, PA-MC-E3, or PA- MCX port adapters.

  Workaround There is no workaround.

- CSCdx88874

  Symptoms An interface may be disabled after a router that has a specific hardware and software configuration is reloaded.

  Conditions This symptom is observed on a Cisco 7206VXR router that has a Network Processing Engine (NPE-400) and that is running Cisco IOS Release 12.2(8)T4.

  Workaround Use a Cisco IOS 12.1 T release.

- CSCdx91957

  Symptoms The **mtu** interface configuration command changes into the **ip mtu** interface configuration command when the VLAN ID changes on a subinterface of a Cisco 12000 series 3-port Gigabit Ethernet line card.

  Conditions This symptom is observed on a Cisco 12000 series Internet router.

  Workaround There is no workaround.

- CSCdy23165

  Symptoms Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) traffic may not pass through a port adapter.

  Conditions This symptom is observed on a Cisco 7500 router that has either a 2-port Fast Ethernet 100BASETX (PA-2FE-TX) or a 2-port Fast Ethernet 100BASE-FX (PA-2FE-FX) port adapter. This symptom is observed when OSPF and EIGRP are configured on either the PA-2FE-TX or the PA-2FE-FX port adapter. The port adapter interface does not form the adjacency because multicast entries are not added to the hardware address filter.

  Workaround Enter the **ip pim** interface configuration command on the port adapter interface to clear the condition.

- CSCdy32609

  Symptoms When the size of the maximum transmission unit (MTU) on an ATM subinterface is modified, the MTU of virtual circuits (VCs) that are configured under that subinterface are set to 0, and the subinterface cannot be pinged.

  Conditions This symptom is observed on a Cisco 7500 router.

  Workaround There is no workaround.

- CSCin10839

  Symptoms A router may reload after a channelized T3 (CT3) port adapter that is configured as part of a Multilink PPP (MLP) bundle is removed, and the MLP bundle interface is shut down.

  Conditions This symptom is observed in a network in which two Cisco 7200 series routers are connected back-to-back via channelized T3 (CT3) port adapters. Channel groups are created and configured for MLP, and a bundle interface multilink is created on both of the routers in this setup.

  Workaround There is no workaround.

IP Routing Protocols

- CSCdu43164

  Symptoms A router may experience a memory leak.

  Conditions This symptom is observed on a Cisco 7206VXR Provider Edge (PE) router that is running Cisco IOS Release 12.1(5a) in a Multiprotocol Label Switching (MPLS)/Virtual Private Network (VPN) network. The memory leak is caused by the Border Gateway Protocol (BGP) I/O process and occurs at the rate of 100 KB to 130 KB per hour (about 2.5 MB to 3 MB per day) after the **show mem sum | incl BGP** privileged EXEC command is entered. This situation occurs regardless of whether the BGP neighbor is flapping.

  The following is command output from the **show proc mem | incl BGP** privileged EXEC command:

  ```
  PID TTY Allocated Freed Holding Getbufs Retbufs Process ... 104 0 3522569548
  2139398320 21965976 297916 5184 BGP I/O ... The show mem sum | incl BGP privileged
  EXEC command shows that function ìBGP (1) updateî allocates memory without
  deallocating it again after the job is completed.

  Router# show mem sum | incl BGP

  Alloc PC Size Blocks Bytes What ... 0x607C42E0 65496 333 21810168 BGP (1) update ....
  ```

  Workaround Reload the PE router.

- CSCdu80977

  Symptoms An external Autonomous System Boundary Router (ASBR) may choose a suboptimal path for an external type 2 route.

  Conditions This symptom is observed on an ASBR router that is situated external to a network that has several Area Border Routers (ABRs).

  Workaround There is no workaround.

- CSCdw45079

  Symptoms A Cisco router may reload if the **clear ip route vrf** *vrf-name* EXEC command is issued on a certain Virtual Private Network (VPN).

  Conditions This symptom is observed on a Cisco 7500 series router that is running the rsp-jsv-mz image of Cisco IOS Release 12.2(6) and that has Multiprotocol Label Switching (MPLS) and VPN enabled.

  Workaround There is no workaround.

- CSCdw52946

  Symptoms When dialing back in to a remote access (RA) service for certain routers, the call setup is successful, but data cannot be transferred because the virtual access interface is removed from the routing table after the call is set up.

  Conditions This symptom is observed when a user attempts to dial back in to a remote access Multiprotocol Label Switching (MPLS)/Virtual Private Network (VPN) service for a Layer 2 Tunneling Protocol (L2TP) dial-in virtual home gateway (VHGW)/provider edge (PE) router and a direct dial-in network access server (NAS)/PE router.

  Workaround There is no workaround.

- CSCdw83531

  Border Gateway Protocol (BGP) updates may be corrupted and the following message may be displayed when this symptom occurs:

  ```
  BGP-6-NEXTHOP: Invalid next hop (0.0.0.0) received from x.x.x.x: martian next hop
  BGP(0): x.x.x.x rcv UPDATE w/ attr: nexthop 0.0.0.0, origin ?, metric 0,
  originator 0.0.0.0, path YYYY, community , extended community
  20.1.1.0/24 -- DENIED due to: martian NEXTHOP;
  ```

  These symptoms are observed on a customer edge (CE) router when BGP updates are sent from a provider edge (PE) router to the CE router when peer groups are specified using the **address-family ipv4 vrf** *vrf-name* router configuration command. BGP routes may be lost on the CE router even though the BGP neighbors remain up.

  Workaround: Remove the peer group configuration from the **address-family ipv4 vrf** *vrf-name* router configuration command

- CSCdx03185

  Symptoms A router may reload when it is searching the Resource Reservation Protocol (RSVP) database.

  Conditions This symptom is observed on a Cisco router that is running in the Route Processor Redundancy Plus (RPR+) or the Stateful SwitchOver (SSO) mode. The router reloads when a tunnel is up and when Multiprotocol Label Switching-traffic engineering (MPLS-TE), Cisco Express Forwarding (CEF), and IP routing are unconfigured using the following sequence of commands:

  ```
  no tag advertise-tags
  no mpls ip
  no mpls label protocol ldp
  ```

```
no ip routing
no ip cef
no mpls traffic-eng tunnels
```

Workaround Issue the **no mpls traffic-eng tunnels** router configuration command to shut down all tunnels before issuing the **no ip routing** global configuration command.

- CSCdx06621

  Symptoms A router may reload with a bus error while the shortest path first (SPF) algorithm is computed.

  Conditions This symptom is observed if multiple routers are advertising the same prefix in Type-5 or Type-7 link-state advertisements (LSAs).

  Workaround There is no workaround.

- CSCdx08399

  Symptoms Lightweight Directory Access Protocol (LDAP) packets may be corrupted.

  Conditions This symptom is observed on a Cisco router when Network Address Translation (NAT) is configured.

  Workaround There is no workaround.

- CSCdx08412

  Symptoms Static routes that are in the process of being downloaded are saved to the startup-config if the **write** command is issued.

  Conditions This symptom occurs if the **write** command is issued while the **aaa route download** global configuration command is executing.

  Workaround Do not issue the **write** command while the **aaa route download** global configuration command is executing.

- CSCdx10820

  Symptoms A router may reload with a bus error.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(7.4).

  Workaround There is no workaround.

- CSCdx10823

  Symptoms An Address Resolution Protocol (ARP) entry is not removed if the **no arp** *ip-address mac-address* global configuration command is issued. The MAC address of the Ethernet interface that has the IP address may be changed.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(7a).

  Workaround Enter the **clear arp** EXEC command after removing a static ARP entry.

- CSCdx17459

  Symptoms A software-forced reload may occur on a router.

  Conditions This symptom is observed on a Cisco 12008 router that has a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel that is configured with an absolute metric when the tunnel is used with the Open Shortest Path First (OSPF) protocol. A watchdog timer event may be triggered, and the router may reload after the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command is issued on the tunnel interface.

  Workaround There is no workaround.

- CSCdx17597

  Symptoms A Multilayer Switch Feature Card (MSFC) and Supervisor Engine may reload during an attempt to format a withdrawn routes message (ìMP_UNREACHî) for that address family. These symptoms have also been observed on a 7500 router.

  Conditions These symptoms are observed on an MSFC and Supervisor Engine that function in a multiprotocol Border Gateway Protocol (MP-BGP) environment with an address family other than the IPv4 unicast address family (such as the IPv4 multicast address family) and with a large number of prefixes in the corresponding BGP table.

  Workaround Remove the address family other than the IPv4 unicast address family.

- CSCdx19396

  Symptoms Addresses that are used for overloading may be used as one-to-one translations.

  Conditions This symptom is observed when a combination of static and dynamic Port Address Translation (PAT) are used, the addresses that are used for overloading may be used as one-to-one translations because for Domain Name System (DNS) packets, the addresses are translated inside the payload. This symptom may cause dynamic translations to fail.

  Workaround Make sure the **ip nat pool inside_pool** contains more than 1 IP address.

- CSCdx25551

  Symptoms A software-forced reload may occur on a router.

  Conditions This symptom is observed on a Cisco router if an interface is shut down from another terminal while output from the **show ip pim neighbor** EXEC command is displayed.

  Workaround There is no workaround.

- CSCdx25807

  Symptoms The **redistribute static route-map** router configuration command does not work correctly if it is issued under a multicast address family.

  Conditions This symptom occurs only if a static route is redistributed into IP version 4 (IPv4) unicast through the network statement and if the static routes are redistributed into multicast using a redistribute statement.

  Workaround Issue the **redistribute static route-map** router configuration command to redistribute the static routes for IPv4 unicast.

- CSCdx32947

  Symptoms When the **ip pim rp-address** *ip-address* [*group-access-list*] [**override**] [*bidir*] global configuration command is configured, a conflict that is learned from an Auto Rendezvous Point (Auto-RP) announcement is still used even if the **override** keyword is specified.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2 S. The router will still accept information from the Auto-RP when this symptom occurs. This symptom will not occur if routers do not have conflicting information.

  Workaround There is no workaround.

- CSCdy32096

  Symptoms Delays, loss of synchronization, and packet loss may be observed with voice or video traffic that is sent over Resource Reservation Protocol (RSVP) ATM switched virtual circuits (SVCs). The SVC quality of service (QoS) parameters indicate a small burst (typically 20 percent of the requested IP burst). This situation causes traffic bursts to be dropped even if the traffic bursts are within the specified burst traffic parameters.

In some cases, the peak cell rate (PCR) and the sustainable cell rate (SCR) may also be lower than what is required for this traffic. The low PCR may cause significant packet loss, video drops, and loss of synchronization between the affected stream and other related streams. The hold queue for the ATM SVC will fill up and remain full for an extended duration.

Conditions This symptom is observed on Cisco 7200 and 7500 routers when voice or video clients are used to generate a stream of small packets.

Workaround There is no workaround.

- CSCdx33019

  Symptoms A router may reload.

  Conditions This symptom is observed when two paths to the same destination network are withdrawn simultaneously.

  Workaround There is no workaround.

- CSCdx38760

  Symptoms A router may reload when configured with a Border Gateway Protocol (BGP) Virtual Private Network (VPN).

  Conditions This symptom has been observed on a Cisco 7500 router.

  Workaround There is no workaround.

- CSCdx42637

  Symptoms A router flushes link-state advertisements (LSAs) that have not been refreshed for more than 50 minutes.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.0(19)ST1.

  Workaround There is no workaround.

- CSCdx48007

  Symptoms The **summary-address** node-level subcommand may not work as expected. If the **summary-address** node-level subcommand is configured on a virtual template, the Enhanced Interior Gateway Routing Protocol (EIGRP) sends out each specific route within the summary address range instead of sending out the summarized routes as configured.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that has a virtual access interface that has a virtual template interface configuration. The Cisco AS5300 is running Cisco IOS Release 12.1 or Release 12.2.

  Workaround Use Cisco IOS Release 12.0(7)T or configure an outbound distribution list to deny the specific routes.

- CSCdx49181

  Symptoms When an additional new area is added to the provider edge (PE), all the type 3 link-state advertisements (LSAs) learned from other PEs via Border Gateway Protocol (BGP) do not get redistributed into this new area.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround Issue the **clear ip ospf redistribution** command.

- CSCdx49744

  Symptoms A link-state advertisement (LSA) may not get flushed from the database.

Conditions This symptom is observed when an LSA is changed from type 3 to type 5.

Workaround Issue the **clear ip ospf x process** command.

- CSCdx53795

  Symptoms If a peer advertises a replacement path (with the same multi-exit discriminator [MED] as the original path), the new path is inserted in the previous position of the original path.

  Conditions This symptom may be observed on a Border Gateway Protocol (BGP) router that is using deterministic MED. When this symptom occurs, the replacement path may not be grouped with paths from the same autonomous system number (ASN). This ordering may result in incorrect routing and may cause routing loops.

  Workaround There is no workaround other than disabling and reenabling deterministic MED on the router after the router enters the incorrect state.

- CSCdx69995

  Symptoms If Border Gateway Protocol (BGP) has more than a few hundred Virtual Private Network version 4 (VPNv4) prefixes to advertise, you may see the following message:

  ```
  %BGP-3-INSUFCHUNKS: Insufficient chunk pools for message, requested size 4204 BGP may
  not be able to advertise the VPNv4 routes.
  ```

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdx70216

  Symptoms A router may reload. Also, a Multilayer Switch Feature Card 2 (MSFC 2) may reload with a bus error in the not so stubby area (NSSA) part of the Open Shortest Path First (OSPF) code.

  Conditions This symptom is observed on any Cisco router that is running a Cisco IOS software release when a link-state advertisement (LSA) with an incontiguous mask is sent to a router.

  Workaround Do not send address LSAs with illegal masks, that is masks that are not contiguous, to a router.

- CSCdx73662

  Symptoms A router may reload because of a bus error after the **show ip sdr** EXEC command is entered.

  Conditions This symptom is observed on a Cisco 7513 router that is running either Cisco IOS Release 12.0(21.1)S2 or Release 12.0(21.3)S1. This symptom occurs because an invalid SDR Session announcement message is received without the name of the session.

  Workaround Avoid the use of the **show ip sdr** command until either the session announcer fixes the problem, or an IOS image with this patch is deployed.

- CSCdx74432

  Symptoms Memory allocation (MALLOC) failures may be observed when Border Gateway Protocol (BGP) updates are generated, and the following error message may be displayed:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of 2093048 bytes failed from 0x602BDB08,
  alignment 0 Pool: Processor Free: 1546596 Cause: Not enough free memory Alternate
  Pool: None Free: 0 Cause: No Alternate pool
  ```

  Conditions This symptom is observed on a Cisco router.

  Workaround There is no workaround.

- CSCdx74764

  Symptoms A performance route processor (PRP) can cause exception when trying to reload the router.

Conditions This symptom is observed on a PRP that is running Cisco IOS Release 12.0(21)3S and that has BGP/Interior Gateway Protocol (IGP) with Multiprotocol Label Switching-traffic engineering (MPLS-TE).

Workaround There is no workaround.

- CSCdx79227

  Symptoms A router may reload after the **show ip mroute summary** EXEC command is entered.

  Conditions This symptom is observed on Cisco router that is running Cisco IOS Release 12.2.

  Workaround There is no workaround.

- CSCdx86289

  Symptoms A memory leak may occur on a router. Background processes, route flapping, and the presence of a large number of routes in the global routing table may expedite the memory leak.

  Conditions This symptom is observed on a Cisco router.

  Workaround Upgrade to the latest Cisco IOS release.

- CSCdy06755

  Symptoms A Border Gateway Protocol (BGP) route cannot be advertised.

  Conditions This symptom is observed on a Cisco 7500 series router that is running the rsp-jsv-mz image of Cisco IOS Release 12.2(11.7).

  Workaround There is no workaround.

- CSCin09989

  Symptoms If a router is reloaded after the **ip rsvp bandwidth** interface configuration command is configured with the default parameters, this command is inadvertently removed from the configuration.

  Conditions This symptom is observed on interfaces that have 75 percent of bandwidth in bps that is not an exact multiple of 1000.

  Workaround Configure the **ip rsvp bandwidth** interface configuration command using explicit parameters.

ISO CLNS

- CSCdw29177

  Symptoms Both the parallel routes may be deleted by Intermediate System-to- Intermediate System (IS-IS) when just one of them is shut down.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.0(20.3)ST when two routers are connected using ATM (tc-atm) parallel links, for example, a1/0.1 and a1/0.2, and the routing protocol is IS- IS. If you shut down a1/0.2, IS-IS deletes both the routes from the routing table even though a1/0.1 is still active.

  Workaround Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM link (a1/0.1).

- CSCdx07428

  Symptoms A router may attempt to establish two pseudonodes on a broadcast adjacency and may create two pseudonodes on the same LAN and cause redundant pseudonode link-state packets (LSPs) to be generated on the network.

Conditions This symptom is observed on a router when the Intermediate System-to-Intermediate System (IS-IS) process restarts before the adjacency on the neighbor router has timed out with the restarted router. This behavior does not properly trigger the designated router (DR) election if the adjacency type is level 1 or level 2.

Workaround Wait until the adjacency becomes inactive before restarting the IS-IS process.

- CSCdx13452

  Symptoms The **timers basic** router configuration command is ignored after a router is reloaded.

  Conditions When this symptom occurs, International Organization for Standardization (ISO)-Interior Gateway Routing Protocol (IGRP) timers are not applied after the router is reloaded.

  Workaround Reenter the **timers basic** router configuration command after the router has reloaded.

Miscellaneous

- CSCdu24618

  Symptoms The “speed 57600” configuration entry may be added to the line configuration on a router.

  Conditions This symptom is observed on a Cisco AS5400 that is running Cisco IOS Release 12.2(5e).

  Workaround Remove the configuration entry from the line configuration.

- CSCdu37284

  Symptoms Previous or initial ping requests disappear from a router.

  Conditions This symptom is observed when ping requests are sent consecutively that is, when a second ping request is created immediately after an initial ping (using the same serial number as the initial ping request).

  Workaround There is no workaround.

- CSCdu45472

  Symptoms A router may display the following message continuously:

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle
  ```

  Conditions This symptom is observed on a Cisco 7200 router that is running Cisco IOS Release 12.1(7)E.

  Workaround Issue the **no ip pxf** global configuration command.

- CSCdu63564

  Symptoms On a router that has static Address Resolution Protocol (ARP) entries configured, the router may fail to use the static ARP entries immediately.

  Conditions This symptom is observed on a Cisco router if CEF is enabled manually or if the router is reloaded with Cisco Express Forwarding (CEF) enabled.

  Workaround Disable CEF on the router by entering the **no ip cef** global configuration command.

- CSCdu65892

  Symptoms An RFC 1577 client may lose its connection to other RFC 1577 clients.

  Conditions This symptom is observed on an ATM interface of a Cisco router. The router does not initiate a new switched virtual circuit (SVC) to restore the lost connectivity.

  Workaround Reset the ATM interface to clear this symptom.

- CSCdv34579

  Symptoms A Versatile Interface Processor (VIP), Gigabit Ethernet Interface Processor (GEIP), Gigabit Ethernet Interface Processor plus (GEIP+), or Packet OC-3 Interface Processor (POSIP) that is installed in a router may reload. The VIP may display the following error message when it reloads:

  ```
  %DMA-1-DRQ_STALLED: DRQ stalled. Dumping DRQ.
  ```

  Conditions This symptom is observed on a Cisco 7500 series router under heavy traffic conditions.

  Workaround There is no workaround.

- CSCdv40244

  Symptoms The following continuous stream of "%POT1E1-3-FWFATAL" error messages may occur on a router:

  ```
  %POT1E1-3-FWFATAL: Bay 5: firmware needsresetdue to fw watchdog timeout
  %POT1E1-3-FWFATAL: Bay 4: firmware needsresetdue to fatal software errors
  ```

  Conditions This symptom is observed on a Cisco 7206VXR router that is running Cisco IOS Release 12.1(8.04) and that is configured with a PA-MC-8T1 port adapter, but may also affect the PA-MC-2T1, PA-MC-4T1, PA-MC-8DSX1, PA-MC- 2E1/120, and PA-MC-8E1/120 port adapters.

  Workaround There is no workaround.

- CSCdv45264

  A universal access server may display the following digital signal processor (DSP) error message:

  ```
  %VTSP-3-DSP_TIMEOUT: DSP timeout on event 6: DSP ID=0x1241: DSP error stats
  ```

  This symptom is observed on a Cisco AS5300 universal access that is used as a voice gateway and that is running Cisco IOS Release 12.2(1a). This symptom has no impact on calls. There is no workaround.

- CSCdv45274

  Symptoms Inaccurate RADIUS acct-input-octets may be generated for IP traffic.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that has an asynchronous interface and that is running Cisco IOS Release 12.2(2). This symptom occurs only if virtual profiles and asynchronous interfaces are used.

  Workaround There is no workaround.

- CSCdv50542

  Symptoms A cable access router may pause indefinitely after it generates the following recurring log message:

  ```
  SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=80B0EE4C, count=0 -Traceback=
  80315D98 8026C6AC 80322A88 803C2540 8042076C 80421110 803C29C0 803C1BA4 80374E10
  ```

  Conditions These symptoms are observed on a Cisco uBR924 cable access router that is running Cisco IOS Release 12.1(5)T9. These symptoms occur if the radio frequency (RF) interfaces reset during an upstream TCP data transfer. The Cisco uBR925 and Cisco uBR905 universal broadband routers, and the Cisco CVA120 cable voice adapter are susceptible to these symptoms.

  Workaround Power-cycle the Cisco uBR924 to bring it back online. Disable selective TCP acknowledgement (ACK) control by issuing the **no ip tcp selective-ack** global configuration command.

- CSCdv56826

  Symptoms E1 channels may remain connected when a call is disconnected from the telephony side.

  Conditions This symptom is observed when the call involves an IP phone and the Cisco Call Manager.

Workaround There is no workaround.

- CSCdv66644

  Symptoms An interactive voice response (IVR) prompt restarts before it is completed. The prompt sounds as though it is disrupted by pauses and static. Sometimes the system replays the prompt and the user hears the same words and phrases several times (stutter).

  Conditions This symptom is observed on a Cisco AS5300.

  Workaround There is no workaround.

- CSCdv75258

  Symptoms In a network that has two Cisco routers, router A handles the first call correctly but clears the second call that is forwarded to it by router B through the Ethernet Layer 2 Forwarding (L2F) protocol.

  Conditions This symptom is observed on two Cisco 3620 routers that are running Cisco IOS Release 12.1(10) and that have Stack Group Bidding Protocol (SGBP) and dialer profiles configured.

  Workaround Configure a virtual template interface and the **multilink virtual-template** command on router A, or use the Cisco IOS Release 12.0 general deployment release.

- CSCdv80024

  Symptoms The T1 controllers on a universal access server may flap periodically when incoming calls are received and may display the following assert messages:

  ```
  from Trunk(1): Assertion Failed: File"../framer/bt8370.c", Line 1282
  from Trunk(1): Assertion Failed: File"../framer/bt8370.c", Line 1288
  ```

  Conditions This symptom is observed on the T1 controllers of a Cisco AS5400 universal access server that is operating in the Extended Superframe (ESF) ATT Facility Data Link (FDL) mode and that is configured for Signaling System 7 (SS7) and PRI signaling.

  Workaround There is no workaround.

- CSCdv86717

  Symptoms An interface may experience an output queue that becomes wedged after a few minutes. The following command output is displayed after the **show interface fast 0/1** EXEC command is entered:

  ```
  FastEthernet0/1 is up, line protocol is up Queueing strategy: fifo Output queue 40/40,
  66826 drops; input queue 0/75, 0 drops
  ```

  Conditions This symptom is observed on a Fast Ethernet or Gigabit Ethernet interface with an i82543 chip that is running Cisco IOS Release 12.2(1).

  Workaround There is no workaround.

- CSCdv86945

  Symptoms The E1 controller displays inaccurate statistics after the **show controllers** [**e1** | **t1**] EXEC command is issued. The following command output shows that the elapsed seconds and the unavailable counters are do not advance:

  ```
  Timestamp - 00:00 E1 3/4 is up. Applique type is Channelized E1 - balanced Framing is
  UNFRAMED, Line Code is HDB3, Clock Source is Line. 0 Errored Secs, 0 Bursty Err Secs,
  0 Severely Err Secs, 270 Unavail Secs 0 Errored Secs, 0 Bursty Err Secs, 0 Severely
  Err Secs, 86400 Unavail Secs

  Timestamp - 01:50 E1 3/4 is up. Applique type is Channelized E1 - balanced Framing is
  UNFRAMED, Line Code is HDB3, Clock Source is Line. 0 Errored Secs, 0 Bursty Err Secs,
  0 Severely Err Secs, 270 Unavail Secs 0 Errored Secs, 0 Bursty Err Secs, 0 Severely
  Err Secs, 86400 Unavail Secs
  ```

Conditions This symptom is observed when an E1 controller is configured for unframed operations using the **controller** {**t1** | **e1**} *slot*/*port* **channel-group 0 unframed** command. The counters are correct when the controller is configured for a Frame Relay operation (CRC-4 or No-CRC4).

Workaround There is no workaround.

- CSCdv89383

  Symptoms Sometimes traffic does not go through both B channels of a hardware advanced interface module-Virtual Private Network (AIM-VPN) module.

  Conditions This symptom is observed when the AIM-VPN is used on a Cisco 2600 router with a BRI.

  Workaround Disable hardware crypto and use software crypto, or use PPP multilink.

- CSCdw09840

  Symptoms Some Service Processing Elements (SPEs) cannot be recovered and remain in the REC PEND state.

  Conditions This symptom occurs after the **spe download maintenance time** global configuration command is issued.

  Workaround Clear the SPEs or issue the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the specific ports.

- CSCdw10866

  Symptoms A router may reload and display traceback messages when the **atm vc-per-vp** interface configuration command is entered.

  Conditions This symptom is observed on a Cisco 3660 router.

  Workaround There is no workaround.

- CSCdw20980

  Symptoms Traffic may fail over static routes.

  Conditions These symptoms have been observed after performing an online insertion and removal (OIR) of a Versatile Interface Processor (VIP) in a Cisco 7500 series router or using the Single Line Card Reload (SLCR) feature after a VIP has reloaded unexpectedly, and if there are static routes defined that use the interfaces on the failed VIP. The traffic that is using those static routes may fail. The static routes include those that are defined within a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) Routing and Forwarding (VRF) instance.

  Workaround Enter the **clear cef linecard** *slot- number* **adjacency** command on the affected VIP.

- CSCdw21153

  Symptoms A Cisco 7500 series router that has the main interface configured as a backup interface and subinterfaces configured using the same IP address may exhibit different bootup behaviors when two Cisco IOS releases are used. When the router is operated, the duplicate IP addresses can be configured in both versions of Cisco IOS software. However, duplicate IP addresses are removed from the configuration in Cisco IOS Release 12.0.

  Conditions The difference in bootup behavior is observed in Cisco IOS Release 11.3(11)WA4(14) and Cisco IOS Release 12.0.

  Workaround Manually configure the affected interfaces again after the router reboots.

- CSCdw27216

  Symptoms Several “RX FIFO was stuck - forced to reset MAC” messages may be logged on the console of a router. This message is specific to port adapters and I/O cards that use a vendor-specific chipset.

  Conditions This symptom is observed on a Cisco 7200 router that is operating in the normal mode. The following is a list of the affected port adapters and I/O cards:

  - 2-port Fast Ethernet 100BASE-TX port adapter (PA-2FE-TX)
  - 2-port Fast Ethernet 100BASE-FX (PA-2FE-FX)
  - Cisco 7200 I/O controller with 2 Fast Ethernet ports (C7200-I/O-2FE/E)
  - Cisco 7200 I/O controller with 2 Gigabit Ethernet ports (C7200-I/O-GE+E)

  Workaround There is no workaround.

- CSCdw31238

  Symptoms A Secure Shell (SSH) client may fail to connect to a router if the router is reloaded with hardware encryption disabled.

  Conditions This symptom is observed on a Cisco 1710 router that has a Virtual Private Network (VPN) hardware encryption module and that has hardware encryption enabled. The SSH client cannot connect to the router after hardware encryption is disabled by issuing the **no crypto engine accelerator** global configuration command after the changes are saved into NVRAM and the Cisco 1710 is reloaded. This symptom occurs only if the **no crypto engine accelerator** global configuration command is issued on the Cisco 1710 while a hardware encryption module is enabled.

  Workaround To prevent this symptom from occurring, do not disable hardware encryption on the Cisco 1710 using the **no crypto engine accelerator** global configuration command while the hardware encryption module is installed on the router.

- CSCdw32424

  Symptoms A personal computer may appear to be connected to both modems in the Address Resolution Protocol (ARP) table. This symptom may persist after the ARP table is cleared and the power on the modem is reset before it is moved. Debug output from the **debug ip dhcp server** privileged EXEC command may indicate that the personal computer is attempting to obtain its IP address. The cable modem termination system (CMTS) first attempts to set the GIADDR field to the primary (cable modem) gateway on the first subinterface before changing the GIADDR field to the secondary gateway personal computer on the correct subinterface. The Dynamic Host Configuration Protocol (DHCP) server log does not show the discover packet using the incorrect GIADDR field.

  Conditions These symptoms are observed on a Cisco uBR7200 universal broadband router that is running Cisco IOS Release 12.1 T or Release 12.1(9)EC. These symptoms occur when a user moves a personal computer from one modem on a subinterface to another modem on a different subinterface.

  Workaround There is no workaround.

- CSCdw35625

  Symptoms A router may reload when an ISDN dialout connection is initiated.

  Conditions This symptom is observed on a Cisco 2500 router that is running Cisco IOS Release 12.2(6.8)T when an ISDN dialout connection is initiated on BRI interface 0.

  Workaround There is no workaround.

- CSCdw39118

  Symptoms A router that is configured with generic routing encapsulation (GRE) tunnels may pause indefinitely and continuously scroll the following messages on the console:

  ```
  %SYS-2-NOTQ: unqueue didnÌt find 0 in queue 62360144 -Process= "<interrupt level>",
  ipl= 1 -Traceback= 60538810 60536468 60536468 6015DB10 60431D64 60433D04 60433DC8
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=0, count=0 -Traceback= 60672220
  60538818 60536468 60536468 6015DB10 60431D64 60433D04 60433 DC8
  ```

  Conditions The conditions under which these symptoms occur are not known at this time.

  Workaround There is no workaround.

- CSCdw41145

  Symptoms When a rotary dial peer is used with the Debit Card 2.0.0 Tool Command Language (TCL), only the first and the last missed rotary attempts are sent to the RADIUS server.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that is running Cisco IOS Release 12.2. This symptom occurs if more than two dial peers are tried in order to reach a destination when the Debit Card feature is used (with each dial peer set to use different priorities). This symptom occurs only if the **aaa accounting connection h323 start-stop radius** global configuration command is configured.

  Workaround There is no workaround.

- CSCdw50839

  Symptoms Packets on a Versatile Interface Processor (VIP) are dropped.

  Conditions This symptom is observed on a Cisco 7500 series router that is configured as a provider edge router in a Multiprotocol Label Switching (MPLS) virtual private network (VPN) switching environment when there are no distributed Cisco Express Forwarding (dCEF) entries for the remote virtual private network routing and forwarding (VRF) route.

  This symptom occurs if a VRF is deleted after dCEF and the Border Gateway Protocol (BGP) are disabled from any previous MPLS VPN configuration.

  Workaround Disable and reenable distributed dCEF by issuing the **no ip cef distributed** global configuration command followed by the **ip cef distributed** global configuration command on the Cisco 7500 series router. End-to-end connectivity is restored after this workaround is performed.

- CSCdw51353

  Symptoms The behavior of the **cable-modem dhcp-proxy nat** *pool-name* cable interface configuration command in Cisco IOS Release 12.2 T is different from the way the command behaves in Cisco IOS Release 12.2 XA4 when a cable modem is changed from bridge mode to another routing mode.

  Conditions An error occurs if the cable modem is removed from the bridge group under the following conditions:

  – Routing is enabled before the cable interface is removed from the bridge group.

  – The cable interface is removed from the bridge group before the Ethernet and the Universal Serial Bus (USB) interfaces are removed from the bridge group.

  This error will leave the cable interface in the bridge group. If this error occurs while the **cable-modem dhcp-proxy nat** *pool-name* cable interface configuration command is configured, the Dynamic Host Configuration Protocol (DHCP) proxy network address translation (NAT) feature will be misconfigured and will not work correctly. The cable interface may also reset if the pool name argument of the **cable-modem dhcp-proxy nat** *pool-name* cable interface configuration command is renewed from DHCP.

Workarounds To change the cable modem from the bridge mode to another routing mode, use one of the following two workarounds:

Workaround A Enable routing only after all interfaces are removed from the bridge group, and configure the no cable-modem compliant bridge interface configuration command on the cable interface. The order in which the interfaces are removed from the bridge group is arbitrary.

Workaround B If routing is enabled, ensure that the Ethernet and the USB interfaces are removed from the bridge group before the cable interface is removed.

To recover from the misconfiguration of the cable-modem dhcp-proxy nat pool-name cable interface configuration command, perform one the following procedures:

- If the configuration has not been saved to NVRAM, reload the cable modem and reconfigure the cable modem using the one of the workarounds above.
- If the configuration has already been saved to NVRAM, clear the NVRAM using the erase startup-config privileged EXEC command, reload the cable modem, and reconfigure the cable modem using one of the workarounds above.

Note If a standard Cisco IOS software configuration is loaded to the running configuration using TFTP or Data-over-Cable Service Interface Specifications (DOCSIS) I/O configuration load, the standard Cisco IOS software configuration must be modified to conform to the workaround.

- CSCdw52216

  Symptoms A High-Speed Serial Interface (HSSI) logical DTE may not recover automatically from a HSSI cable fault. The transmission data light on the HSSI DTE may be unlit when this symptom occurs. The HSSI DTE may appear to be transmitting Local Management Interface (LMI) enquiries, but no LMI updates are received from the Frame Relay switch. Command output from the **debug frame-relay lmi** EXEC command may indicate that LMI inquiries are sent out from the router but the interface is not receiving any LMI updates from the Frame Relay switch.

  Conditions This symptom is observed on a HSSI on a router if the HSSI cable between the CSU and the HSSI interface is unplugged and then plugged back in after the HSSI interface is declared to be in the down state.

  Workaround Issue the **clear interface hssi** EXEC command on the logical HSSI DTE.

  Alternate Workaround Issue the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the logical HSSI DTE.

- CSCdw53085

  Symptoms A router may reload with the following error message:

  ```
  System was restarted by bus error at PC 0x60A9DBF8, address 0xD0D0D2D at Image
  text-base: 0x60008950, data-base: 0x61542000 0x60A9DBF8 x60A9DF38 0x60A8AC18
  0x60A8B1D8 0x60A8B374 0x603FC5B4 0x603FC5A0
  ```

  This error manifests itself only upon bootup. Once the router is up and running, this bus error never happens.

  Conditions This symptom is observed on a Cisco 7140 router that is running the c7100-io3s-mz.121-12 image of Cisco IOS Release 12.1(12).

  Workaround There is no workaround.

- CSCdw55259

  Symptoms A Cisco 2600 series router with a High Density Voice Network Module (NM-HDV) reloads because of a bus error and displays an error message similar to the following message when the **show version** command is entered:

  ```
  System returned to ROM by bus error at PC 0xXXXXXXXX, address 0xYYYYYYYY at 00:32:45
  UTC Tue May 21 2002
  ```

  In the error message example, 0xXXXXXXXX represents the program counter where the reload happens, and 0xYYYYYYYY represents the address where the router reloads.

  Additionally, it has been observed that a Cisco 2600 series router with a NM-HDV installed may reload when the router is booted. Once the router is up and running, this bus error never happens.

  Conditions These symptoms have been observed on a Cisco 2600 series router with a NM-HDV module.

  Workaround There is no workaround. For more information about bus errors, refer to the following document:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml

- CSCdw56539

  Symptoms A subinterface configuration is removed from the **standby track** privileged EXEC command after a reload.

  Conditions This symptom is observed on a Cisco 2600 router that is running Cisco IOS Release 12.2(6) and Release 12.2(7). This symptom occurs when the Hot Standby Router Protocol (HSRP) is configured to track an ATM inverse multiplexing over ATM (IMA) subinterface.

  Workaround Perform one of the following workarounds:

  - Manually configure the ATM IMA subinterface by entering the **standby track** interface configuration command after reloading the router. This workaround assumes that the ATM IMA main interface is defined in the configuration.
  - Configure the main ATM IMA interface by entering the **standby track atm1/ima0** interface configuration command and configure the ATM IMA 0.1 interface by entering the **standby track atm1/ima0.1 50** interface configuration command.

- CSCdw58439

  Symptoms The locIfSlowOutPkts Simple Network Management Protocol (SNMP) counter may go backwards when an SNMP walk is performed.

  Conditions This symptom is observed on a Cisco 3600 router that is running Cisco IOS Release 12.2(5a).

  Workaround There is no workaround.

- CSCdw59988

  Symptoms If the **busyout forced** voice-port configuration command is issued on a channel-associated signaling (CAS) voice port during an active call, the call is disconnected. No new outgoing calls can be made even after the **no busyout forced** voice-port configuration command is issued on the voice port.

  Conditions This symptom is observed on a Cisco 3600 router that is running Cisco IOS Release 12.2 T.

  Workaround Issue the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the CAS T1 controller or the CAS voice port.

- CSCdw60124

  Symptoms If an ATM tag switching subinterface is created and the multi-virtual circuit (Multi-VC) mode is enabled on the subinterface, the local prefixes of a label distribution protocol (LDP) neighbor do not appear in the label forwarding table if the subinterface is deleted and subsequently recreated.

  Conditions This symptom is observed on a Cisco router that has a Route Switch Processor (RSP4).

  Workaround Reload the router.

- CSCdw60179

  Symptoms IP traffic may not go through a router that has a Virtual Private Network (VPN) card enabled.

  Conditions This symptom is observed on a Cisco 3640 router that is running Cisco IOS Release 12.2(7.5) and that has IP Security (IPSec) and generic routing encapsulation (GRE) configured with either Cisco Express Forwarding (CEF) or CEF flow switching on a VPN card.

  Workaround Use an alternate switching type or use transforms that have a smaller encapsulation size.

- CSCdw61066

  Symptoms Modem ISDN channel aggregation (MICA) technologies modules may become bad and later recover without either the use of modem recovery or any user intervention.

  Conditions This symptom occurs under normal conditions in which calls are received and disconnected at a regular 30-minute intervals.

  Workaround There is no workaround.

- CSCdw61734

  Symptoms Modem ISDN channel aggregation (MICA) technologies modems may pause indefinitely and display a ìVDEV_STATUS_ACTIVE_WDTî status after the **show modem csm** EXEC command is issued.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that has MICA modems and that is running Cisco IOS Release 12.2(6).

  Workaround There is no workaround.

- CSCdw64685

  Symptoms When a high density voice network module (NM-HDV) is configured for a channel group that is used for data connectivity to conduct voice calls, users may experience poor voice quality.

  Conditions This symptom is observed on an NM-HDV that is installed on a Cisco 3600 router that is running Cisco IOS Release 12.2 or Release 12.2 T and that has High-Level Data Link Control (HDLC) or Multilink PPP (MLP) configurations.

  Workaround There is no workaround.

- CSCdw67032

  Symptoms Operation, Administration, and Maintenance (OAM) cells may be delayed in transmission, and OAM cells may be sent out of sequence.

  Conditions This symptom is observed on an overloaded permanent virtual circuit (PVC). The PVC may go down when this symptom occurs.

  Workaround There is no workaround.

- CSCdw67237

  Symptoms A router may log the following error message:

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

CPU utilization is consumed by the call management process and may increase to 99 percent.

Conditions This symptom is observed on a Cisco 3620 router that is configured for analog modem calls.

Workaround There is no workaround.

- CSCdw68693

  Symptoms An incorrect sequence of H.323 and Q Signaling (QSIG) messages is displayed on a router after a call is placed to a busy extension.

  Conditions This symptom is observed in the debug trace output of a Cisco 3620 router that is configured as an outgoing gateway. When a call is placed from phone A to a busy phone (phone B) through the Cisco 3620, an ISDN disconnect message followed by a disconnect message are found in the debug trace output even though the terminating PBX has not issued a connect message.

  Workaround Force the call to use H.323 slow start procedures.

- CSCdw69768

  Symptoms A headend edge label switch router (ELSR) may generate unsynchronized tag bindings and display the following error message:

  ```
  %SCHED-3-THRASHING: Process thrashing on watched managed timer (0x414A4920).
  -Process= "TC-ATM Proc", ipl= 4, pid= 88 -Traceback= 40398AC0 40398EC0 4099DF14
  ```

  Conditions These symptoms are observed in a cell-based Multiprotocol Label Switching (MPLS) setup. These symptoms are observed on the headend ELSR after the tailend of an ELSR tag distribution protocol (TDP) or label distribution protocol (LDP) session is toggled. These symptoms occur because the headend ELSR does not clean up all tag bindings completely after the TDP or LDP session goes down. The headend ELSR keeps the state of some of the stale tag bindings as active.

  Workaround When this symptom occurs, the user can toggle the headend TDP or LDP session by issuing the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command either on the extended tag ATM (XTagATM) interface on the label switch controller (LSC) or on the MPLS subinterface on the headend ELSR.

- CSCdw70156

  Symptoms A router may reboot unexpectedly after it is configured for Voice over ATM (VoATM) calls.

  Conditions This symptom is observed on a Cisco 3660 router that is running Cisco IOS Release 12.2(2)XB. This symptom does not affect Voice over IP (VoIP) or Voice over Frame Relay (VoFR) calls.

  Workaround Configure a permanent virtual circuit (PVC) with a virtual path identifier (VPI) value that is less than 64.

- CSCdw70293

  Symptoms Systems Network Architecture Switching Services (SNASw) may not release memory as expected.

  Conditions This symptom is observed on a Cisco 2600 router that is running SNASw and that is running Cisco IOS Release 12.2(6). The router may consume memory in a two-network node servers scenario in which one of the servers has failed and recovered. The SNASw directory services process is the process that consumes memory.

  Workaround There is no workaround.

- CSCdw70494

  Symptoms CPU utilization may reach 100 percent at about 22 Mbps of traffic for four tunnels.

  Conditions This symptom is observed when multiple IP Security (IPSec)/Generic Routing Encapsulation (GRE) tunnels use Frame Relay encapsulation on a Cisco 7200 series router.

  Workaround Use PPP and High-Level Data Link control (HDLC) encapsulation to improve the performance for a single tunnel.

- CSCdw72724

  Symptoms A router may pause indefinitely when it is reloaded.

  Conditions This symptom is observed on a Cisco 3660 router that is running Cisco IOS Release 12.2(8)T after the router is reloaded.

  Workaround Power-cycle the Cisco 3660.

- CSCdw75607

  Symptoms When IP level IP Security (IPSec) encryption is used, inbound packets may be dropped and messages such as "CRYPTO-4-RECVD_PKT_INV_SPI" that indicate that the contents of the packets are invalid may be displayed.

  Conditions These symptoms are observed in configurations that have IPSec running on a Multilink PPP (MLP) bundle interface and when the multilink peer is generating very small fragments. If the peer segments an IPSec frame into fragments whereby the entire IPSec header is not contained within the first fragment, local IPSec processing may fail after the local multilink engine passes the reassembled IPSec datagram up to the IPSec level. In general, these symptom may occur on any system in which IPSec frames are transported by a link type that supports some form of link-level fragmentation. Other example setups in which these symptoms may occur may include Frame Relay multilink or IP-within-IP tunnels such as virtual private dial-up network (VPDN) in which the inner IP layer is carrying IPSec frames but additional IP fragmentation is occurring at the outer IP layer.

  Workaround If the user has control over the peer system and is able to configure the method of fragmentation on the peer, the user should configure the peer system so that the entire IP and IPSec header is contained within a single fragment. When MLP bundle is used, issue the **ppp multilink fragment-delay** *milliseconds* interface configuration command on the peer system to configure the amount of fragment delay that should be present on the MLP bundle. Alternatively, the fastswitching of IP traffic on interfaces that carry IPSec traffic may be disabled.

- CSCdw75655

  Symptoms A label switch controller (LSC) may reboot.

  Conditions This symptom is observed when more than 3800 label virtual circuits (LVC) and permanent virtual circuits (PVCs) are created from a label edge router (LER).

  Workaround There is no workaround.

- CSCdw76822

  Symptoms IP connectivity may be disrupted after distributed Cisco Express Forwarding (dCEF) is configured on a router.

  Conditions This symptom is observed on a Cisco 7500 series router that is functioning as a provider edge (PE) router and that is running tag switching or Multiprotocol Label Switching (MPLS). This symptom occurs if the router is running both cell-based and frame-based tag switching simultaneously.

  Workaround There is no workaround.

- CSCdw79992

  Symptoms A Cisco router displays traceback messages similar to the following message:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x601606E4 reading 0x38C
  %ALIGN-3-TRACE: -Traceback= 601606E4 60160A7C 6037F298 605F3A54 605F8240 605F6FD0
  605F9208 605F28AC
  ```

  Conditions This symptom has been observed on Cisco 2600, 3600, 3745 and 7200 series routers with BRI interfaces and hardware compression.

  Workaround There is no workaround.

- CSCdw82241

  Symptoms After a multiprotocol external Border Gateway Protocol (MP-eBGP) update, if you enter the **show mpls forwarding-table** command, the VPN labels that are shown do not match the VPN labels that are shown if you enter the **show ip bgp vpnv4 all** command.

  Conditions This symptom is observed in a network configuration with the following characteristics:

  – Several Cisco 12000 series Internet routers function as provider (P) and provider edge (PE) routers. At least one Cisco 12000 series Internet router functions as a PE autonomous system border router (ASBR).

  – All Cisco 12000 series Internet routers are configured with 8-port Packet over SONET (POS) and 3-port Gigabit Ethernet line cards. - The routers function in an interautonomous system Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment.

  Workaround Enter the **clear ip bgp *** command on the router that functions as the PE-ASBR.

- CSCdw87882

  Symptoms When a high density voice network module (NM-HDV) is configured for a channel group that is used for data connectivity to conduct voice calls, users may experience poor voice quality.

  Conditions This symptom is observed on an NM-HDV that is running Cisco IOS Release 12.2 or Release 12.2 T with Multilink PPP (MLP) configurations.

  Workaround There is no workaround.

- CSCdw90486

  Symptoms Differentiated services code point (DSCP) or type of service (ToS) based class-based weighted fair queueing (CBWFQ) traffic classification may not work with hardware accelerator cards.

  Conditions This symptom is observed on a Cisco 2600 router that is using an advanced integration module (AIM) Virtual Private Network (VPN) card and that has CBWFQ, IP Security (IPSec), and generic routing encapsulation (GRE) enabled. The Cisco 2600 is running Cisco IOS Release 12.2(7a). The same configuration works normally if software encryption is used.

  Workaround Use Cisco IOS Release 12.2(2)T or a later release.

  Alternate Workaround Use process switching.

- CSCdw92846

  Symptoms Dangling digital signal processors (DSPs) may occur on a universal access server.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that is configured as both an outgoing gateway (OGW) and a terminating gateway (TGW) and that is running Cisco IOS Release 12.2(6). The number of dangling DSPs remains in the dangling state and continues to increase as time passes. This symptom occurs only if there is no matching dial peer for the calls that are coming in from the ISDN side.

  Workaround Ensure that there are matching dial peers for calls that originate from the ISDN side.

- CSCdw93047

  Symptoms Packet losses may occur for pings to and from a router.

  Conditions This symptom is observed on a Cisco 7200 series router with hardware encryption or Unicast Reverse Path Forwarding (URPF).

  Workaround Disable Unicast Reverse Path Forwarding or remove the hardware encryption module.

- CSCdw93958

  Symptoms A software-forced reload may occur on a Node Route Processor (NRP).

  Conditions This symptom is observed on a Cisco 6400 NRP when the NRP runs low on buffer memory.

  Workaround There is no workaround.

- CSCdw94336

  Symptoms Reverse Address Resolution Protocol (RARP) packets are not bridged from an ATM interface to the Fast Ethernet interface.

  Conditions This symptom is observed on the ATM and Fast Ethernet interfaces on a Cisco router.

  Workaround There is no workaround.

- CSCdw94532

  Symptoms A router may experience digital signal processor (DSP) timeouts and show an error message similar to the following error message:

  ```
  CET: dsp 6 is not responding CET: dsp 14 is not responding
  ```

  Conditions This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(6a) or Release 12.2(9).

  Workaround There is no workaround.

- CSCdw94847

  Symptoms The call success rate (CSR) degrades about 5 percent when a Tool Command Language (TCL) 1.0 debit card script is used in a busy network environment.

  Conditions This symptom is observed on a Cisco AS5800 universal access server that is running Cisco IOS Release 12.2(7a) or 12.2(7b). Several calls are disconnected unexpectedly when this symptom occurs. This symptom may be caused by a slow response from the RADIUS server when calls are set up and torn down at the same time.

  Workaround Use a faster RADIUS server.

- CSCdw95464

  Symptoms A universal access server may reload because of a bus error when analog calls are made.

  Conditions This symptom is observed on a Cisco AS5800 universal access server that is running Cisco IOS Release 12.2(2)XB05.

  Workaround There is no workaround.

- CSCdx01664

  Symptoms A router may fail to obtain an IP address via the Dynamic Host Configuration Protocol (DHCP).

  Conditions This symptom is observed on a Cisco 806 router that is running Cisco IOS Release 12.2(8)T if a DHCP server does not send the subnet mask option in the DHCP OFFER message.

  Workaround There is no workaround.

- CSCdx02036

  Symptoms If the prefix of a provider edge (PE) router is learned over a Packet over SONET (POS) interface, the prefix is untagged.

  Conditions This symptom is observed in a Carrier Supporting Carrier (CsC) topology in which two Cisco PE routers are connected to a POS interface. The prefix of the PE router is untagged after the topology is configured if the prefix is learned over a POS interface. When this symptom occurs, traffic forwarding through the CsC core is stopped.

  Workaround Manually clear the prefix from the routing table and establish a tag for the prefix.

- CSCdx05010

  Symptoms A Route Processor Module (RPM) interface may not work after it is reloaded.

  Conditions This symptom is observed on a Cisco MGX8250 RPM if two or more subinterfaces are configured with the same ATM permanent virtual connection (PVC) name that uses identical characters for the first 15 characters.

  Workaround Configure ATM PVC names that are unique and that have 15 characters or less.

  When the Cisco MGX8250 is first configured, multiple subinterfaces can be configured with a PVC that is 15 characters if the characters are unique. However, if the first 15 characters are identical after a reload, other subinterfaces fail because only one subinterface retains the PVC statement.

- CSCdx05682

  Symptoms A modem may display "%MODEM-3-MODEMOOS: Modem number 2/40 is marked oos" messages.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that is running Cisco IOS Release 12.2(2)XA4. The modems are running firmware version 2.9.1.0. This symptom occurs if the modem accepts a call because the modem could not be marked as "out of service."

  Workaround Apply a modem cap entry to the running configuration and configure the **modem autoconfigure type** line configuration command on the line interfaces.

- CSCdx05828

  Symptoms The voice gateway loses the second digit of an information message and calls an incorrect number.

  Conditions This symptom occurs if, during overlap receiving on a Cisco voice gateway that is running Cisco IOS Release 12.2(6b) or Release 12.2(9)S, the information message carries two digits and the call setup message has a progress indicator (PI) value of three. If the call setup message does not have a PI, all digits are collected correctly.

  Workaround There is no workaround.

- CSCdx05883

  Symptoms It is not possible to strip off the progress indicator (PI).

  Conditions On a Cisco voice gateway you can modify the PI value in an alerting message by using the **progress_ind alert enable** *pi-number* command (where the *pi-number* argument has a value of 1, 2, or 8) on the outgoing dial peer of the terminating gateway, but it is not possible to strip off the PI entirely.

  Workaround There is no workaround.

- CSCdx06026

  Symptoms A router may reload when a multilink option is unconfigured from a virtual template on a router.

Conditions This symptom is observed on a Cisco router that is using Multilink PPP over ATM (MLPoATM) and that is running Cisco IOS Release 12.2. The router reloads when a multilink option is unconfigured from the virtual template.

Workaround Delete the ATM permanent virtual circuit (PVC) or shut down the interface on which the PVC is configured before unconfiguring the multilink on the PVC.

- CSCdx06532

  Symptoms A Simple Network Management Protocol (SNMP) get request on the MIB object pnniLinkIfIndex that is defined in the Private Network-Network Interface MIB (PNNI-MIB) module returns “0”.

  Conditions This symptom is observed on PNNI interfaces of Cisco ATM switches. The symptom does not occur on virtual path tunnel interfaces.

  Workaround There is no workaround.

- CSCdx07627

  Symptoms A gateway may appear to send back (echo) the nonstandard data that is received in an H.225 call signaling message to the sender when an H.245 message is tunneled in a H.225 facility message.

  Conditions This symptom is observed on an H.323 gateway that is running Cisco IOS Release 12.2(6). If dual tone multifrequency (DTMF) relay is enabled, the gateways have to exchange the H.245 terminal capability set (TCS) message even though the call is a faststart call. When a H.245 message is tunneled using an H.225 call signaling channel, the received nonstandard data parameter from the other gateway is reencoded and sent back.

  Workaround Use slowstart calls that have a separate H.245 connection.

- CSCdx08414

  Symptoms Some variables for the ATM-MIB are not supported or do not function as expected.

  Conditions This symptom is observed on the Cisco 1400 and Cisco 2600 router.

  Workaround There is no workaround.

- CSCdx08455

  Symptoms A mobile node that is running on a router may stop receiving traffic after the mobile node roams away from a Home Agent (HA) and Foreign Agent (FA) combination to another FA.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2 or 12.1.

  Workaround Clear the visitor entry that corresponds to the mobile node on the HA and FA combination after the mobile node registers with the new FA.

- CSCdx09217

  Symptoms A router that has a Virtual Private Network (VPN) advanced interface module (AIM) may not boot properly after the router is reloaded if the router contains the **no crypto engine accelerator** global configuration command in the configuration.

  Conditions This symptom is observed on a Cisco 2600 router that has a VPN-AIM.

  Workaround Configure the **crypto engine accelerator** global configuration command before reloading the router.

- CSCdx09654

  Symptoms Network Address Translation (NAT) is not reset if Parallel Express Forwarding (PXF) is enabled.

Conditions This symptom is observed on a Cisco 7200 router when NAT is used while PXF is enabled. An NAT entry is created when the data flow starts. The NAT entry is then switched by PXF with active data that is going through the translation. The data flow does not reset the timeout timer and sessions may be dropped as a result.

When the configured timeout value is reached, the packets are punted back to the CPU for a new NAT entry. The new entry has different translation information and may cause the session to assume that the session is new causing the old session to be terminated.

Workaround Extend the timeout values.

- CSCdx10170

  Symptoms A router may stop replying to Address Resolution Protocol (ARP) requests.

  Conditions This symptom is observed on a Cisco router that is used as the active Hot Standby Router Protocol (HSRP) router for certain HSRP groups. The router may stop replying to ARP requests that are sent to the IP address of the HSRP. This symptom occurs only if HSRP is configured on more than one interface.

  Workaround Configure the **no standby redirects** global configuration command on the HSRP router.

- CSCdx11366

  Symptoms The maximum number of modular quality of service (MQC) command-line interface policy maps on a router is limited to 256.

  Conditions This symptom is observed on a Cisco 7200 router that is running Cisco IOS Release 12.2(8)T. CSCdv64193 imposed the restriction on the maximum number of policy maps that can be issued on a router to 256.

  Workaround Use Cisco IOS Release 12.2 T or Release 12.2(8)T1. In Cisco IOS Release 12.2(8)T1 and Release 12.2 T, the maximum number of policy maps that can be configured on a platform is based on what a given platform can support.

- CSCdx12501

  Symptoms A switch VLAN may come up when its first port comes up. If there is a delay in subsequent switch ports coming up in the same VLAN, a Hot Standby Router Protocol (HSRP) group on that VLAN may become active before receiving any packets from other HSRP groups on the subnet. If HSRP PREEMPT is not configured, this behavior is unexpected.

  Conditions This symptom is observed when configuring HSRP between two CATALYST 6000 switches that are running Cisco IOS Release 12.1(8b)E9 and when removing PREEMPT from the configurations of the respective VLANs.

  Workaround Configure longer HSRP Hold and Hello timers.

- CSCdx13597

  Symptoms A router reloads when you enter the **show tag-switching tdp neighbors** command.

  Conditions The conditions under which these symptoms occur are not known at this time.

  Workaround There is no workaround.

- CSCdx13852

  Symptoms The **disc_pi_off** voice port configuration command does not work as expected on the Foreign Exchange Office (FXO) or Foreign Exchange Station (FXS) ports on a router. When a disconnect message with a progress indicator (PI) is received, the router does not clear or disconnect the call.

Conditions This symptom is observed on a Cisco router that is running Cisco IOS version 12.2(10) or an earlier release. This symptom is observed when FXS-to-Voice over IP (VoIP) H.323 calls or FXO-to-VoIP H.323 calls are made. The call clears automatically after 30 seconds or after the calling party hangs up.

Workaround There is no workaround.

- CSCdx14343

  Symptoms A processor may reload.

  Conditions This symptom is observed on a Route Switch Processor (RSP) and Versatile Interface Processor (VIP) when toggling between the **no ip cef distributed** global configuration command and the **ip cef distributed** global configuration command or the **no tag-switching ip** global configuration command and the **tag-switching ip** global configuration command. This situation has been observed when egress NetFlow is configured.

  Workaround There is no workaround.

- CSCdx14383

  Symptoms A SYS-2-CHUNKEXPANDFAIL may occur when an E1 controller uses E1-R2 signaling with the below messages:

  ```
  %SYS-2-CHUNKEXPANDFAIL: Could not expand chunk pool for VTSP EVENT pool. No memory
  available -Process= "Chunk Manager", ipl= 3, pid= 4 -Traceback= 6033D4E4
  %VTSP-3-NOEVENT: no free event structure available from vtsp_ev_chunk_pool for DSP
  message
  ```

  Conditions This symptom is observed on an E1 controller that is installed on a Cisco AS5300 universal access server that is running Cisco IOS Release 12.2(7). This symptom can be verified by examining the command output of the **show chunk | beg vtsp** EXEC command:

  ```
  1320 8 2276 537 0 537 0 VTSP EVENT pool 0x618CC5C8 1320 8 713180 537 0 537 0 (data)
  0x622BCA58 32 0 852 20 0 20 4 Call Management 0x6182D0D0
  ```

  The value 0 (5th column from left - ElementInUse) indicates the number of voice telephony security parameter (VTSP) EVENT chunks that are in use. This value should be 0 if no calls are present (as in the case of the command output that is shown above). This value changes according to the number of active calls. A continuous increase of this value indicates that VTSP EVENT memory is not being released, eventually resulting in chunk memory allocation (MALLOC) failures.

  Workaround There is no workaround other than reloading the box

- CSCdx14794

  Symptoms A modem call does not send data after the data send ready (DSR) signal comes up on the modem.

  Conditions This symptom is observed on a Cisco AS5800 universal access server that has a Cisco AS5800 series 324-port card that has a Cisco NextPort modem. The client side may keep sending PPP and Link Control Protocol (LCP) frames until a timeout occurs.

  Workaround There is no workaround.

- CSCdx16376

  Symptoms A router may reload because of a bus error and display the following message when the **show version** EXEC command is issued:

  ```
  System returned to ROM by bus error at PC 0xXXXXXXXX, address 0xXXXXXXX
  ```

  Conditions This symptom is observed on a Cisco AS5800 universal access server that is running T1 channel-associated signaling (CAS) or the E1 R2 protocol under a heavy load.

  Workaround There is no workaround.

- CSCdx16714

  Symptoms A Route Processor (RP) may experience a bus error or pause indefinitely when a crash test is performed.

  Conditions This symptom occurs after the **test crash** command is issued on an active RP.

  Workaround Reload or power-cycle the router.

- CSCdx17573

  Symptoms Multiprotocol Label Switching (MPLS) does not update the Cisco Express Forwarding (CEF) table with the new local tags after a Route Processor Redundancy Plus (RPR+) cutover occurs.

  Conditions This symptom is observed on a Cisco 7500 Route Processor (RP) that is running Cisco IOS Release 12.0 S.

  In a dual RP system, the standby RP acts as a line card to the primary RP, and all Forwarding Information Base (FIB) and Tag Forwarding Information base (TFIB) entries are downloaded to the standby RP. Because the label distribution protocol (LDP) is also running on the standby RP, the LDP makes all the rewrites on the tag_info command field to be NULL. After an RPR+ cutover occurs, the FIB does not trigger the TFIB to delete the tag_info command field because the FIB does not detect a nontrivial change. Because of this behavior, the TFIB is associated with invalid and NULL entries.

  Workaround There is no workaround.

- CSCdx19436

  Symptoms Overlap calls may fail under certain circumstances.

  Conditions This symptom occurs if no additional digits are received in ISDN INFO messages after the initial setup. The call is rejected even though an outgoing dial peer exists to route the call using the called number in the setup.

  Workaround There is no workaround.

- CSCdx19855

  Symptoms A router may reload.

  Conditions This symptom is observed during the execution of the **no e1 1 channel-group 0** command on the controller of a Multi-Channel E3 port adapter on a Cisco 7200 series router that is configured for IP routing.

  Workaround Shut the interface down and then remove the channel group.

- CSCdx20393

  Symptoms The **busyout monitor** voice port configuration command may be triggered incorrectly.

  Conditions This symptom is observed on a voice port that is configured to monitor two or more local router interfaces (such as Ethernet, Fast Ethernet, or serial interfaces). The busyout condition is triggered if any of the interfaces (other than the first listed interface) is in the “DOWN” state. The voice port oscillates between the in-service and the busyout conditions until all monitored interfaces are active again.

  Workaround There is no workaround.

- CSCdx20802

  Symptoms Memory fragmentation may cause 2 MB of memory allocation to fail.

  Conditions This symptom affects edge routers that are configured for multi-virtual circuit (Multi-VC) and that have Label-Controlled ATM (LC-ATM) interfaces connected toward a Multiprotocol Label Switching (MPLS) core.

  Incremental memory leaks occur after the LC-ATM interface is toggled by issuing the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command or after Cisco Express Forwarding (CEF) is enabled and later disabled on the router by issuing the **ip cef** global configuration command followed by the **no ip cef** global configuration command. Incremental memory leaks may also be seen when route flaps occur. If the incremental memory leaks continue, memory fragmentation may occur and traffic may stop passing through the LC-ATM interface.

  Workaround There is no workaround.

- CSCdx20871

  Symptoms Packets get stuck in Rx ring of the Fast Ethernet.

  Conditions This symptom is observed on a Cisco 1720 router when a long packet comes into the controller.

  Workaround Enter the clear interface command so that the input packet can be recognized.

- CSCdx20996

  Symptoms A router may reload if a configuration is changed.

  Conditions This symptom is observed on a Cisco router that is running tag distribution protocol (TDP) or label distribution protocol (LDP). The reload occurs when TDP or LDP is unconfigured.

  Workaround There is no workaround.

- CSCdx21092

  Symptoms Voice telephony security parameter (VTSP) table errors may be observed when a mixed variety of voice calls (such modem relay, fax relay, and fax pass-through) are tested. The voice port may be in the “seized” state on the terminating gateway.

  Conditions This symptom is observed on a Cisco 3600 series router.

  Workaround There is no workaround.

- CSCdx22225

  Symptoms A low connect rate occurs when a vendor-specific client uses the Layer 2 Tunneling Protocol (L2TP) to establish a virtual private dial-up network (VPDN) connection.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(7). There is only a 60-percent call connect rate when this symptom occurs.

  Workaround There is no workaround.

- CSCdx24321

  Symptoms An asynchronous modem call may not come up.

  Conditions This symptom is observed on a Cisco AS5800 universal access server that is running Cisco IOS Release 12.2(9.4).

  Workaround Use Cisco IOS Release 12.2(9.3).

- CSCdx24750

  Symptoms A Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel may assume an outgoing link that is different from the one that is specified in the explicit path if the outgoing link of the TE tunnel fails.

  Conditions This symptom is observed in an MPLS TE tunnel that is set up explicitly by specifying the IP address of the next hop interface as the next address. This symptom occurs if the outgoing IP address is a router ID.

  Workaround There is no workaround.

- CSCdx24817

  Symptoms Inbound traffic on the Fast Ethernet channel may not be switched via distributed Cisco Express Forwarding (dCEF), but via CEF on the Route Switch Processor (RSP). This may cause high CPU utilization when migration from the Fast Ethernet interface to the Fast Ethernet channel occurs.

  Conditions This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2(6), Release 12.2(7b), or Release 12.2(9)S and that has a Fast Ethernet channel configured on a Versatile Interface Processor (VIP) with a PA-2FE-ISL port adapter.

  Workaround Use a PA-2FE-TX port adapter.

- CSCdx25471

  Symptoms A Cisco AS5800 router shelf (RS) reloads after a Service Processing Element (SPE) module has reloaded.

  Conditions This symptom is observed on a Cisco AS5800 that is configured with a Universal Port Card using NextPort software.

  Workaround There is no workaround.

- CSCdx25843

  Symptoms A router may reload.

  Conditions This symptom is observed when a dynamic crypto map is configured with an access control list (ACL) that has 50 access control entries (ACEs). This symptom occurs only if the router is configured using TFTP using the **copy run tftp** command or from a disk.

  Workaround Do not configure the router using TFTP or from a disk. Use the console to configure the router.

  Alternate Workaround Lower the number of ACEs in the ACL that is used by the dynamic crypto map.

- CSCdx26331

  Symptoms The call-history information that is generated by the Session Initiation Protocol (SIP) call leg does not have a valid duration (nonzero) even though the plain old telephone service (POTS) call history for the same call has a nonzero duration.

  Conditions This symptom is observed when the acknowledge (ACK) message fails to reach the terminating gateway (TGW).

  Workaround There is no workaround.

- CSCdx29222

  Symptoms Input errors (aborts) and output errors (underruns) may occur on a network module.

Conditions These symptoms are observed on an 8-port asynchronous/synchronous network module (NM-8A/S) that is installed on a Cisco 3662 router that is running Cisco IOS Release 12.2(1b). These symptoms occur if the Cisco 3662 has either a 2-port serial WAN interface card (WIC-2T) or a 2-port asynchronous/synchronous WAN interface card (WIC-2A/S) installed and only if the interfaces are enabled. These symptoms do not occur after the shutdown interface configuration command is issued on the WIC-2T or WIC-2A/S interface. WAN interface cards are installed on the 1-port 10/100 Ethernet 2 WAN card slot network module (NM-1FE2W), the 1-port 10/100 Ethernet 1 4/16 Token Ring 2 WAN card slot network module (NM-1FE1R2W), the 2-port 10/100 Ethernet 2 WAN card slot network module (NM-2FE2W), and the 2-port WAN card slot network module (NM-2W). These symptoms are observed only when multicast traffic is present.

Workaround Enter the **shutdown** interface configuration command on the WIC-2T or WIC-2A/S interface.

- CSCdx29607

  Symptoms The **unbundle** privileged EXEC command is not recognized.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that is running Cisco IOS Release 12.2.

  Workaround There is no workaround.

- CSCdx30790

  Symptoms During periods of low traffic, a router may lose its multicast route (mroute) forwarding table and no longer be able to forward packets out of an interface.

  Conditions This symptom is observed on a Cisco 7200 series router. The number of interfaces that exhibit this symptom increases in proportion to the duration of time that the router encounters a low-traffic volume.

  Workaround Enter the **clear ip mroute *** EXEC command or the **clear ip mroute group-name** EXEC command.

- CSCdx31544

  Symptoms Active reverse Telnet sessions on a preconfigured port on a network module may stop transmitting data if the **physical-layer async** interface configuration command is configured on another port.

  Conditions This symptom is observed on an 8-port asynchronous/synchronous network module (NM-8A/S) that has the **physical-layer async** interface configuration command configured on one port.

  Workaround Do not configure the **physical-layer async** interface configuration command on a port if any of the ports on the network module has an active session. Clear the active lines before configuring the **physical-layer async** interface configuration command. Alternatively, the router can be reloaded after the command is configured.

- CSCdx32573

  Symptoms When fragmented User Datagram Protocol (UDP) packets are encrypted using a port-based access control list (ACL), the packets are not flow-switched even if Cisco Express Forwarding (CEF) is configured.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(6f).

  Workaround There is no workaround.

- CSCdx33691

  Symptoms An Enterprise Extender (EE) link to a host may toggle between the up and the down states.

Conditions This symptom occurs when the physical unit (PU) link is not predefined on the host or when the PU is predefined as "DISNCT=xxx" rather than "DISNCT=NO." When this symptom occurs, the incorrect value for the ALIVE timer is passed between the two Real-Time Transport Protocol (RTP) endpoints in a connection setup.

Workaround Predefine the PU link on the host as "DISCNT=NO."

- CSCdx34225

  Symptoms A Systems Network Architecture Switching (SNASw) router may reload in the routine ntl_avl_rotate_right. Traceback contains the following message:

  ```
  0x6104B57C:nba_mmcpu_compare_proc_type(0x6104b578)+0x4 0x61143930:ntl_avl_find
  (0x611438f8)+0x38 0x6104B00C:nba_update_mm_stats(0x6104af6c)+0xa0
  0x611472B8:nba_mm_free(0x61147294)+0x24 0x61144F98:nba_free_buffer(0x61144f00) +0x98
  0x61147C2C:nba_send_ips(0x61147a78)+0x1b4 0x61140888:nbm_free_buffer
  (0x61140818)+0x70 0x61147C3C:nba_send_ips(0x61147a78)+0x1c4
  ```

  Conditions This symptom is observed when two downstream Low Entry Nodes (LEN) send Berkeley Internet Name Domains (BINDs) with the same Procedure Correlation Identifier (PCID) correlator at the same time. This situation should be a very rare occurrence, but some devices may use a random number when generating PCID correlators.

  Workaround There is no workaround.

- CSCdx34255

  Symptoms NVRAM becomes very busy after the **write memory** EXEC command is entered to store a very large configuration. A vty session may appear to be active after the TCP session has ended. Neither the vty session nor the line can be cleared. Memory allocation (MALLOC) failures may occur on the slave Route Switch Processor (RSP).

  Conditions These symptoms are observed on a router that has master and slave cards if a very large configuration is stored using the **write memory** EXEC command on the master card.

  Workaround Reload the slave RSP using the slave console port.

- CSCdx34351

  Symptoms The Open Settlements Protocol (OSP) does not try all destinations that are returned from the OSP server. When an OSP server returns multiple destinations in the AuthorizationResponse message, a gateway does not attempt to set up the call using one of the destinations until a call is successful or until the list is exhausted.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that is used as an outgoing gateway and that is running Cisco IOS Release 12.2(9.2). If a terminating gateway fails to validate the token from a call that is made from the outgoing gateway, the outgoing gateway stops and does not attempt to set up the call to the second destination or report source usage indication.

  Workaround There is no workaround.

- CSCdx35300

  Symptoms A Gigabit Ethernet input queue may become wedged.

  Conditions This symptom is observed on a Cisco 7400 router.

  Workaround There is no workaround.

- CSCdx36117

  Symptoms A microcode reload of a 3-port Gigabit Ethernet (GE) line card causes the Forwarding Information Base (FIB) to be disabled and the following error message to be displayed:

  ```
  %FIB-3-FIBDISABLE: Fatal error, slot 2: No window message, LC to RP IPC is no
  n-operational
  ```

Conditions This symptom is observed after a Border Gateway Protocol (BGP) convergence of a Cisco 12416 Internet router that is running Cisco IOS Release 12.0(21.2)S and that is configured with 200 BPG peers and the following line cards:

- Two 8-port or 16-port OC-3 Packet-over-SONET line cards (in a shutdown state)
- Four 3-port GE line cards, each configured with an even distribution of 2000 VLAN subinterfaces
- Three 6-port channelized T3 line cards (in a shutdown state)
- Two Quad OC-12 ATM line cards (in a shutdown state)

Workaround There is no workaround.

- CSCdx36647

  Symptoms If the *value* argument of the **server trigger destination-info** *value* gatekeeper configuration command is configured with a value such as "800*", the value is interpreted and reported correctly by Cisco IOS software but the "*" character is lost in NVRAM after the running configuration is saved and cannot be seen when the **show running-config** EXEC command is issued.

  Conditions This symptom is observed on a Cisco gatekeeper.

  Workaround Instead of saving the running configuration, copy the correct configuration from a file to the startup configuration. When this step is performed, the "*" character is not shown when the **show running-config** EXEC command is issued but the "*" character will be interpreted correctly by Cisco IOS software. The output of the **show gatekeeper servers** EXEC command can be used to check if the system is working with the correct prefixes. The output of the **show startup-config** EXEC can be used to verify that NVRAM contains the correct configuration. Ensure that NVRAM contains a good configuration.

- CSCdx37171

  Symptoms A router sends T-protocol data units (T-PDUs) to the incorrect User Datagram Protocol (UDP) port.

  Conditions This symptom is observed on a Cisco General Packet Radio Service (GPRS) support node (GGSN) that is running Cisco IOS Release 12.2(8.4). This symptom occurs if two different serving GPRS support nodes (SGSNs) are included for data and signaling in the create request.

  Workaround There is no workaround.

- CSCdx37849

  Symptoms A device that is running Cisco IOS software may reload when a command is issued to display a file that contains certain character patterns.

  Conditions This symptom occurs if the file in question has a very large line. This line may have a very large continuous set of characters without any new line characters and is most likely corrupted.

  Workaround There is no workaround.

- CSCdx38290

  Symptoms A router may reload.

  Conditions This symptom is observed on a Cisco 7200 series router and on the Node Route Processor (NRP2) of a Cisco 6400 series switch when two virtual circuit (VC) classes that involve variable bit rate non-real time (VBR-NRT) parameters from two separate Telnet sessions are modified.

  Workaround There is no workaround.

- CSCdx38578

  Symptoms An edge router reloads when route flapping occurs.

  Conditions This symptom is observed on an edge router that has the Multi-VC feature configured and that has an label-controlled ATM (LC-ATM) interface that faces the Multiprotocol Label Switching (MPLS) core.

  Workaround There is no workaround.

- CSCdx38690

  Symptoms Large packets cannot be passed on a router that has a High-Speed Serial Interface (HSSI) module.

  Conditions This symptom is observed on an HSSI network module that is installed on a Cisco 3600 router that is running Cisco IOS Release 12.2(10) or Release 12.2(10.3)T.

  Workaround Issue the **mtu 1019** interface configuration command to set the maximum transmission unit (MTU) size of the HSSI interface to 1019 bytes. This workaround may not work in all cases.

- CSCdx39383

  Symptoms A failure cause code may change from the terminating gateway (TGW) to the originating gateway (OGW). The same cause code is not propagated back from the TGW to the OGW.

  Conditions This symptom is observed with tandem-switched calls in a tandem-switched Voice over Frame Relay (VoFR) network that has a Cisco 3600 router that is running Cisco IOS Release 12.2(5).

  Workaround There is no workaround.

- CSCdx39412

  Symptoms A gateway may use an incorrect cause code value to release calls that are disconnected because of the expiration of the Real-Time Transport Control Protocol (RTCP) timer.

  Conditions This symptom is observed on a Cisco AS5300 universal access gateway that has the RTCP timer feature enabled by issuing the **timer receive-rtcp** *timer* gateway configuration command to detect and release idle calls.

  Workaround There is no workaround.

- CSCdx40311

  Symptoms CISCO-GATEKEEPER-MIB (.1.3.6.1.4.1.9.10.40.2.1) traps are sent with incorrect gateway IP address information.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(5d).

  Workaround There is no workaround.

- CSCdx40496

  Symptoms A router may release a call with an incorrect cause code of 0x3F.

  Conditions This symptom is observed on a Cisco 3600 router that is running Cisco IOS Release 12.2(5).

  Workaround There is no workaround.

- CSCdx42779

  Symptoms A router may reload unexpectedly when the **show service-module** EXEC command is entered for one of the channels of a T1 controller, and an output similar to the following may be displayed:

  ```
  %ALIGN-1-FATAL: Corrupted program counter pc=0xA, ra=0xXXXXXXXX, sp=0xYYYYYYYY
  %ALIGN-1-FATAL: Corrupted program counter pc=0xA, ra=0xXXXXXXXX sp=0xYYYYYYYY
  Unexpected exception, CPU signal 10, PC = 0xA **** 0xXXXXXXXX is the representation
  of "ra" 0xYYYYYYYY is the representation of "sp" 0xA is the representation of "pc"
  ```

  Conditions This symptom is observed on a Cisco router that has a 2-Port T1 Multiflex Trunk interface card (VWIC-2MFT-T1) that is housed in a network module card that has an integrated DSU/CSU.

  Workaround Avoid entering the **show service-module** EXEC command on interfaces that do not have integrated DSUs.

- CSCdx43071

  Symptoms Various errors may be reported by the Integrated Service Adapter (ISA). The ISA microcode may also pause indefinitely.

  Conditions This symptom is observed on an ISA of a Cisco router that is running Cisco IOS Release 12.2(10.3)T or Release 12.2(10.3)T1.

  Workaround There is no workaround.

- CSCdx43540

  Symptoms Advanced Technology Attachment (ATA) boot requests may be halted.

  Conditions This symptom is observed on ATA Flash cards.

  Workaround There is no workaround.

- CSCdx43636

  Symptoms Incorrect Low Latency Queueing (LLQ) and Weighted Random Early Detection (WRED) statistics may be observed on a router when the **show policy-map interface** *interface-name* EXEC command is entered.

  Conditions This symptom is observed on a Cisco router while there are hundreds of virtual circuits (VCs) on the router.

  Workaround There is no workaround.

- CSCdx43902

  A c7200 router with NSE-1 processor may fail to boot when loading a c7200-p-mz image.

- CSCdx45205

  Symptoms Open Shortest Path First (OSPF) fails across a multilink bundle.

  Conditions This symptom is observed in a distributed Multilink PPP (dMLP) configuration that has N links in a multilink bundle when a Cisco 7500 router is setup back-to-back with any other peer router. When any of the links are removed from the bundle on one side (other than Cisco 7500), OSPF connectivity is lost for few seconds on the Cisco 7500 router side and then recovers immediately.

  Workaround There is no workaround.

- CSCdx45298

  Symptoms A Cisco Express Forwarding (CEF) inconsistency may occur between a Gigabit Route Processor (GRP) and an Engine 2 line card. This inconsistency may cause flapping.

  Conditions This symptom is observed when there are recursive prefixes and when the line quality is suboptimal.

  Workaround Clear the CEF line card.

- CSCdx45332

  Symptoms Internet Key Exchange (IKE) may fail to generate Diffie-Hellman values.

  Conditions This symptom is observed on a Cisco 7500 series router that has a Versatile Interface Processor (VIP) interface and that is running Cisco IOS Release 12.2(6c).

  Workaround There is no workaround.

- CSCdx45679

  Symptoms A router reloads when packets are process switched from the IP to the Multiprotocol Label Switching path and need to be fragmented.

  Conditions The conditions under which these symptoms occur are not known at this time.

  Workaround There is no workaround.

- CSCdx47143

  Symptoms Some E1 controller ports may remain down after a router is booted up.

  Conditions This symptom is observed on a Cisco AS5800 access concentrator that is running Cisco IOS Release 12.2(2)XB5.

  Workaround Enter the **shutdown** interface command followed by the **no shutdown** interface configuration command on the E1 controller that has paused indefinitely in the down state.

- CSCdx47342

  Symptoms A Cisco 12008 Internet router reloads because of a bus error and displays the following error message:

  ```
  System returned to ROM by bus error at PC 0x5037FD38, address 0x34303A41
  ```

  Repeat usage of the **show mpls forwarding** command or the **show tag forwarding** command causes the router to reload.

  Conditions These symptoms are observed on a Cisco 12008 Internet router that is running the gsr-p-mz image of Cisco IOS Release 12.0(21)ST1 and occur because of a string overflow in a local stack. This string overflow occurs because the Virtual Private Network version 4 (VPNv4) prefixes in the autonomous system border router (ASBR) use the complete IP address as the route distinguisher (for example, “rd: 138.xxx.xxx.xxx:0”) when the **show tag forwarding** command is typed, instead of the much shorter autonomous system number.

  Workaround Define the route distinguishers using autonomous system numbers instead of IP addresses.

- CSCdx47521

  Symptoms A Systems Network Architecture Switching Services (SNASw) router that is configured with a downstream port of conntype=len incorrectly advertises itself as nodetype=NN in the exchange identification (XID) exchange.

  Conditions This symptom is observed on SNASW routers that are running Cisco IOS Release 12.0 T, 12.1 and 12.2.

  Workaround There is no workaround.

- CSCdx47693

  Symptoms A Systems Network Architecture Switching Services (SNASw) dependent logical unit requester (DLUR) router cannot activate the pipe between the DLUR and the dependent logical unit server (DLUS). The following message may be displayed on the router:

  ```
  **** 00001202 - EXCEPTION 512:492 (0) **** Locate search failed: search error Sense
  code = 0x08900060 Origin CP name = XXXXXXXX.XXXXXX Origin LU name = XXXXXXXX.XXXXXX
  Destination LU name = YYYYYYYY.YYYYYY
  ```

  Conditions This symptom is observed on an SNASw router that is running Cisco IOS Release 12.2(6).

  Workaround Restart the SNASw protocol by issuing the **snasw stop** privileged EXEC command followed by the **snasw start** privileged EXEC command on the router.

- CSCdx47760

  Symptoms An interface may lose a statically configured IP address.

  Conditions This symptom is observed if the **shutdown** interface configuration command is entered on an interface after the interface is configured with an IP address by entering the **ip address** *ip-address* [*subnet-mask*] interface configuration command.

  Workaround Reconfigure the static IP address on the interface. The **shutdown** interface configuration command can be issued after the static IP address is configured on the interface.

- CSCdx55493

  Symptoms A router may pause indefinitely if an installed cable interface resets repeatedly.

  Conditions This symptom is observed on a cable modem interface that is installed on a Cisco uBR900 series router. The Cisco uBR900 has to be power-cycled to be returned to normal working condition.

  Workaround There is no workaround.

- CSCdx56527

  Symptoms A router may reload after a memory leak occurs.

  Conditions This symptom is observed on any Cisco router that is running Cisco IOS Release 12.2 (or 12.2B or 12.2T). The memory leak is triggered by authentication, authorization, and accounting (AAA) when AAA attempts to enable TCP header compression twice within the same user session.

  Workaround Disable TCP header compression when a RADIUS or AAA database is used.

- CSCdx56694

  Symptoms The h323-disconnect-time attribute records a time in the telephony STOP record that is approximately 2 seconds different from the time that is recorded in the same attribute in the Voice over IP (VoIP) STOP record.

  Conditions This symptom is observed on a Cisco network access server (NAS) that is running Cisco IOS Release 12.2(10.3)T2.

  Workaround There is no workaround.

- CSCdx56779

  Symptoms A router may reload with the following error message after the watchdog restarts when H.323 firewall inspection is used:

  ```
  WATCHDOG: Process aborted on watchdog timeout, process = IP Input.
  ```

Conditions This symptom is observed on a Cisco router that is running the c7100-io3s-mz image of Cisco IOS Release 12.2.

Workaround There is no workaround.

- CSCdx57538

  Symptoms IP security (IPSec) traffic occurs intermittently over an IPSec generic routing encapsulation (GRE) tunnel.

  Conditions This symptom is observed when you use a hardware encryption card in Cisco IOS Release 12.2(7a) or Release 12.2(7b). The IPSec GRE tunnel itself works fine.

  Workaround There is no workaround.

- CSCdx57803

  Symptoms A router may generate traceback messages after the **clear crypto sa** EXEC command is entered.

  Conditions This symptom is observed on a Cisco 7500 series router that has a Versatile Interface Processor (VIP). This symptom does not impact the service of the router.

  Workaround There is no workaround.

- CSCdx58489

  Symptoms A router may reload if the **clear ip mobile binding all** EXEC command is entered while the **no service alignment detection** global configuration command is configured and the **ip mobile home-agent** global configuration command is not configured.

  Conditions This symptom is observed on a Cisco router if the **ip mobile home-agent** global configuration command is not configured.

  Workaround To prevent the router from reloading, enable service alignment detection, or configure the **ip mobile home-agent** global configuration command.

- CSCdx58649

  Symptoms This caveat relates to issues discovered when a vendor-specific PBX is tested with a Catalyst 8540 switch using ATM switched virtual circuits (SVCs). The following is a listing of symptoms and caveats that relate to signaled ATM point-to-multipoint (P2MP) connections and the issues that are specific to ATM P2MP connections on a Catalyst 8540 switch:

  – Hardware processing to release connection IDs virtual path identifier (VPI)/virtual circuit identifier (VCI) on a low-rate P2MP connection may be slow. When the add-party or the drop-party statements are issued in quick succession on such a connection, insufficient time is allowed to elapse, and an add party may be unnecessarily rejected.

  – When a slave Network-to-Network Interface (NNI) node (in terms of connID allocation) proposes a connection to the master, the master uses the proposed VPI/VCI to give the slave proposed virtual circuit (VC) another connID. Two SVCs own the same underlying VC and may cause a dangling half-leg and allocate bandwidth that is not returned.

  – ATM signaling messages that have unexpected values in the second byte of the ATM signaling message type are dropped. This behavior is incorrect.

  – Several debug messages that are received during error debugging are normal events. This behavior may cause the log buffer to be clogged with nonerror messages such as “mmc errors” and “atm sig cc-errors.”

  Conditions The symptoms above relate to signaled ATM P2MP connections and the issues that are specific to ATM P2MP connections on a Catalyst 8540 switch.

  Workaround There is no workaround for any of the symptoms listed above.

- CSCdx59068

  Symptoms Multilink PPP (MLP) load balancing and quality of service (QoS) mechanisms do not work properly on a Cisco router.

  Conditions Multilink PPP (MLP) load balancing and QoS mechanisms may not work properly on the Cisco 2600, Cisco 3600, Cisco 3700, and Cisco VG200 series routers, except for MLP bundles whose member links lie exclusively on interfaces provided by Cisco high density voice network modules (NM-HDVs).

  Workaround There is no workaround.

- CSCdx61632

  Symptoms If there is a sequence mismatch between peer routers that have an interconnected multilink interface, the recovery sequence for the router that is out of synchronization may take an extended period of time and may affect the traffic that is on the router.

  Conditions This symptom is observed on a Cisco 7500 series router that is running Multilink PPP (MLP).

  Workaround Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected multilink interface.

- CSCdx62533

  Symptoms A Cisco 7500 series router reloads with an error message that is similar to the following:

  ```
  rx_intr: Received giant packet -- dsize=4488, max=4488, p_count=10, max_p_count=9
  ```

  Conditions This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.0(21.3)S1 and that is configured with a PA-SRP- OC12MM port adapter.

  Workaround There is no workaround.

- CSCdx62857

  Symptoms A ring-no-answer call is disconnected after 3 minutes. This symptom occurs regardless of the setting that is used in the **timeouts ringing** {*seconds* | **infinity**} voice-port configuration command.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(10).

  Workaround There is no workaround.

- CSCdx63762

  Symptoms Received packets are discarded when the sequence number of crypto map instances exceeds 100000. When this symptom occurs, the "%CRYPTO-4-RECVD_PKT_INV_IDENTITY_ACL: ipsec check access: identity not allowed by ACL" error message is displayed in the log.

  The following command output is displayed when the **show crypto map** privileged EXEC command is entered:

  ```
  Router# show crypto map Crypto Map "XXX" 100080 ipsec-isakmp <<=== Peer = x.x.x.x Peer
  = y.y.y.y Extended IP access list access-list permit ip any 10.101.5.184 0.0.0.7
  dynamic (created from dynamic map RLAD/10) Current peer: y.y.y.y Security association
  lifetime: 4608000 kilobytes/3600 seconds PFS (Y/N): Y DH group: group1 Transform
  sets={ XXX-SET, }
  ```

  The following command output is displayed when the **show crypto sa** privileged EXEC command is entered:

  ```
  Router# show crypto sa
  ```

```
Level 1: local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0) remote ident
(addr/mask/prot/port): (10.101.5.184/255.255.255.248/0/0) current_peer: y.y.y.y
PERMIT, flags={} #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0 #pkts decaps: 11,
#pkts decrypt: 11, #pkts verify 11 #pkts compressed: 0, #pkts decompressed: 0 #pkts
not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0 #send errors 0,
#recv errors 11 <<===
```

Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(8)T.

Workaround There is no workaround.

- CSCdx63798

  Symptoms A network access server (NAS) port may prepend for the acct-sess-id (44) attribute that is missing when the radius-server attribute nas-port format d global configuration command is enabled.

  Conditions This symptom is observed only when a Node Switch Processor (NSP) cross-connect virtual circuit (VC) is active before the Node Route Processor (NRP) boots up and before the permanent virtual circuits (PVCs) are created.

  Workaround Ensure that the NRP is reloaded if NSP cross-connect VCs are changed.

- CSCdx65232

  Symptoms A memory allocation (MALLOC) failure may occur on a router.

  Conditions This symptom is observed on a Cisco router when an H.323 call is set up during a fax load.

  Workaround There is no workaround.

- CSCdx66907

  Symptoms When a line enters the EM_PARK state, the router starts a 10-second timer. After the 10 seconds have elapsed, the router sends an answer signal of 1 second. The line demultiplexer (demux) that provides the Foreign Exchange Station (FXS) lines recognizes this answer signal and applies a battery reversal over the line. This battery reversal provokes the public accounting systems to charge a 1-second call.

  Conditions This symptom is observed on a Cisco 2600 series router that has a Cisco VG200 voice gateway and that is using recEive and transMit (E&M) under any one the following conditions:

  - When the called number is busy and the calling party remains off-hook.
  - When the calling party hangs up the phone and does not dial any number (or does not complete dialing the number) and remains with the phone off-hook.
  - When the subscriber shakes the hook and causes the line to enter the EM_PARK state.

  Workaround There is no workaround.

- CSCdx66919

  Symptoms The **destination-pattern** {*ldn* | **not-provided**} interface configuration command accepts capital letters as a valid string. This is an incorrect command behavior because the command should not accept capital letters.

  Conditions This symptom is observed on a voice dial peer.

  Workaround There is no workaround.

- CSCdx67033

  Symptoms The “destination out of order” cause code is not passed transparently in a network.

Conditions This symptom is observed in a network that is using ISDN, Voice over IP (VoIP), H.323, and Voice over Frame Relay (VoFR).

Workaround There is no workaround.

- CSCdx67602

  Symptoms An indefinite output pause may occur on a serial interface that is a member of a multilink group, and the following logs may be seen:

  ```
  %RSP-3-RESTART: interface Serial3/0/0, not transmitting Serial3/0/0 : microcode
  reload
  ```

  Conditions This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2(10) with a PA-4T-V35 port adapter inserted in the Versatile Interface Processor (VIP)2-50 or in the VIP2-40 and where one physical interface is a member of a multilink group and another interface is configured for High-Level Data Link Control (HDLC), and where Cisco Express Forwarding (CEF) is enabled globally and disabled on the multilink interface (bundle master), and, lastly, where distributed weighted fair queuing (WFQ) is enabled on the interface configured for HDLC.

  Workaround There is no workaround.

- CSCdx68097

  Symptoms A NextPort Software Port Entity (SPE) module may pause indefinitely in the download mode after the **clear spe** EXEC command is entered. When nondefault firmware is used, a similar symptom is observed and no calls can be made.

  Conditions This symptom is observed on a NextPort SPE module of a Cisco router that is running Cisco IOS Release 12.2(10a).

  Workaround There is no workaround.

- CSCdx69032

  Symptoms Deny statements on an access list that are attached to dynamic crypto maps are ignored if there is already an existing IP Security (IPSec) security association (SA).

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2 and that has Tunnel Endpoint Discovery (TED) enabled.

  Workaround There is no workaround.

- CSCdx69045

  Symptoms A router may reload because of a bus error.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.1 E or Release 12.2 and that is configured to run Cisco Appliance Services Architecture (CASA).

  Workaround There is no workaround.

- CSCdx69748

  Symptoms A router resets itself five minutes after reaching the “maintenance state.”

  Conditions This symptom is observed on a Cisco uBR925 cable access router that is running the k8boot image.

  Workaround Set the lease renewal time to a duration that is longer than 5 mins using the Cisco Network Registrar (CNR). If the lease renewal time is set to a duration of 5 minutes, the Cisco uBR925 may not stay up long enough to allow a new image to be downloaded.

- CSCdx69889

  Symptoms Packet forwarding difficulties may be observed on a Cisco router.

Conditions This symptom is observed on a Cisco router that is acting as a Layer 2 Tunneling Protocol (L2TP) network server (LNS). This symptom occurs on the Multiprotocol Label Switching (MPLS) interface when the router is forwarding packets from the MPLS interface to L2TP tunnels while Cisco Express Forwarding (CEF) is enabled. This symptom does not occur if CEF is disabled on the interface and if the packets are process-switched.

Workaround Disable CEF on the MPLS interface or enable debugging for MPLS packets.

- CSCdx73145

  Symptoms Spurious memory access may be observed with the vp_ipfib_fixup process.

  Conditions The symptom is observed on a Cisco router that has a Route Switch Processor (RSP).

  Workaround There is no workaround.

- CSCdx75775

  Symptoms The multicast prefix 224.0.0.0/4 is missing from the Cisco Express Forwarding (CEF) table for all nondefault Virtual Private Network (VPN) routing/forwarding (VRF) instances on all line cards and redundant Route Processors.

  Conditions This symptom is observed on a a Cisco 12000 series Internet router.

  Workaround There is no workaround.

- CSCdx75835

  Symptoms The watchdog timer may time out when IP traffic is sent over an interface using X.25 encapsulation.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(10.8).

  Workaround There is no workaround.

- CSCdx76632

  Symptoms A Cisco AS5300 that is functioning as a voice gateway may reload because of an incoming bus error exception.

  Conditions This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(6d).

  Workaround There is no workaround.

- CSCdx76907

  Symptoms A Versatile Interface Processor (VIP4-80) may reload with a bus error when distributed Multilink PPP (dMLP) is configured.

  Conditions This symptom occurs when traffic is passed through the dMLP bundle and occurs just after the interface comes up. This symptom is specific to the dMLP feature and will occur only if dMLP is configured on a platform. The dMLP feature is independent of other features and does not affect other features.

  Workaround There is workaround.

- CSCdx78215

  Symptoms Packets that are sent by a router using hardware encryption over a Multilink PPP (MLP) link may be dropped at the other end of the IP Security (IPSec) tunnel.

  Conditions This symptom is observed on a Cisco 1700 series router that has a Virtual Private Network (VPN) module installed and that is running Cisco IOS Release 12.2(8.5)T.

  Workaround Use process switching, or disable the hardware crypto engine (VPN module).

- CSCdx80891

  Symptoms If policing is enabled using the modular quality of service QoS command-line interface CLI (MQC), it may not work with Class-Based Weighted Fair Queueing (CBWFQ) on a Frame Relay subinterface, although it may work properly with Low Latency Queueing (LLQ).

  Conditions This symptom is observed on a Cisco 7500 series router when packets are Cisco Express Forwarding (CEF) switched instead of distributed Cisco Express Forwarding (dCEF) switched. Also, if output policing is enabled on the router, output policing and output queueing may not work.

  Workaround Disable output policing, or make sure that packets are dCEF switched instead of non-dCEF switched.

- CSCdx81251

  Symptoms A Route Switch Processor (RSP) may reload when a Frame Relay map class is applied at the permanent virtual circuit (PVC) level on a Frame Relay interface.

  Conditions This symptom is observed on a Cisco 7500 series router in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) environment. This symptom will not occur if the Frame Relay interface does not have a Virtual Private Network (VPN) routing/forwarding (VRF) instance configured.

  Workaround Enter the **no fair-queue** interface configuration command at the interface level, and apply the map class at the PVC level.

  Alternate Workaround A Insert the map class at the interface level.

  Alternate Workaround B Enter the **no fair-queue** command, enter the **fair-queue** command again, and reapply the map class at the PVC level.

- CSCdx82069

  Symptoms A Cisco AS5400HPX cannot be booted with any image. The following messages appear on the console:

  ```
  rommon 3 > boot bus error while trying to access flash - addr = 0xb8000000 cannot read
  flash info getdevnum warning: device "boot flash" has size of zero bus error while
  trying to access flash - addr = 0xb8000000 cannot read flash info getdevnum warning:
  device "boot flash" has size of zero open: read error...requested 0x4 bytes, got 0x0
  trouble reading device magic number boot: cannot open "bootflash:" boot: cannot
  determine first file name on device "bootflash:" rommon 4 >
  ```

  Conditions These symptoms are observed on a Cisco AS5400HPX that is running Cisco IOS Release 12.2(7.4) or a later 12.2 release.

  Workaround There is no workaround.

- CSCdx84445

  Symptoms A line card may be stuck in the off-for-download state.

  Conditions This symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(21)S2. This symptom may be indicated in the output of the **show cef linecard** EXEC command.

  Workaround There is no workaround.

- CSCdx87079

  Symptoms A Voice over IP (VoIP) call may cause a terminating gateway to reload.

  Conditions This symptom is observed on a Cisco AS5400 universal gateway that is running Cisco IOS Release 12.2(11)T under certain VoIP configurations.

  Workaround There is no workaround.

- CSCdx88731

  Symptoms The dial string that is passed for a V.110 callback may become corrupted, and dialout will stop working.

  Conditions This symptom is observed on a Cisco AS5300 universal access server when the dial string is appended with two more digits. This symptom affects only V.110 callbacks.

  Workaround There is no workaround.

- CSCdx88897

  Symptoms Label distribution protocol (LDP) cannot create a Tag Information Base (TIB) entry for 0.0.0.0, which prevents LDP from performing label switching on a packet that is routed using the default route.

  Conditions This symptom is observed in Cisco IOS Release 12.2(11.03)T, Release 12.2(11.03)S, Release 12.2(011.003), Release 12.0(21.04)SY, and Release 12.0(21.04)S.

  Workaround There is no workaround.

- CSCdx89427

  Symptoms A router may reload when priority queueing is removed from a service policy.

  Conditions This symptom is observed on a Cisco 7200 series router that is running an image of Cisco IOS Release 12.2.

  Workaround There is no workaround.

- CSCdx90805

  Symptoms It may not be possible to make H.323 fax calls.

  Conditions This symptom is observed on a Cisco AS5850 universal gateway when the Resource Reservation Protocol (RSVP) is configured.

  Workaround There is no workaround.

- CSCdx91806

  Symptoms A router may reload with a bus error when a high density voice network module (NM-HDV) disconnects a call.

  Conditions This symptom is observed on a Cisco 2600 series, Cisco 3600 series, or a Cisco 3700 series router that has an NM-HDV. This symptom is observed in Cisco IOS Release 12.2(11.3), Release 12.2(11.3)T, and Release 12.2(11.3)S. This symptom affects channel-associated signaling (CAS) voice ports and ISDN voice ports.

  Workaround There is no workaround.

- CSCdx93079

  Symptoms The first information frame of the user logical unit-logical unit (LU-LU) session is sent with both the source MAC address and the destination MAC address in the noncanonical (Token Ring) format.

  Conditions This symptom is observed if Systems Network Architecture Switching Services (SNASw) is configured with High Performance Routing (HPR) Logical Link Control, type 1 (LLC1) frame over data-link switching (DLSw) for the uplinks and if Ethernet is used for the downstream connection. This symptom will occur regardless of whether the downstream port uses the address of the Ethernet interface or the address of the Hot Standby Router Protocol (HSRP) interface. This symptom does not occur if the downstream port is a Token Ring, virtual Token Ring, or virtual data-link control (VDLC) port. This symptom does not occur if the uplink uses LLC2 port definition.

  Workaround There is no workaround.

- CSCdx95071

  Symptoms Outgoing ISDN calls may be terminated, and the following error message may be displayed:

  ```
  0x80AF - Resource unavailable, unspecified
  ```

  The "bad" state is indicated in the "CURR STATE" column of the output from the show voice dsp EXEC command if the command is entered when this symptom occurs.

  Conditions This symptom is observed on a Cisco 3640 router that is running Cisco IOS Release 12.2(10a).

  Workaround There is no workaround.

- CSCdy04411

  Symptoms Under rare circumstances, a Channelized T3 (CT3) card may reboot because of a bus error and then recover. The router itself does not reboot or reload; just the card by itself.

  Conditions This symptom is observed when the CT3 card is installed on a Cisco AS5850 that is running Cisco IOS Release 12.2(2)XB6.

  Workaround There is no workaround.

- CSCdy06569

  Symptoms A call may fail to connect when there is an incoming E1 R2 call that has to be resource-switched.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that is running Cisco IOS Release 12.2.

  Workaround There is no workaround.

- CSCdy07131

  Symptoms A router may not complete the Dynamic Host Configuration Protocol (DHCP) autoinstall process.

  Conditions This symptom is observed on a Cisco router that does not have a nonvolatile memory (NVM) startup configuration.

  Workaround There is no workaround.

- CSCdy09165

  Symptoms Security association (SA) traffic may not be passed on certain platforms.

  Conditions This symptom is observed on a Cisco 805 or Cisco 4500 series router after Internet Key Exchange (IKE) is established. This symptom is observed with preshare and Rivest, Shamir, and Adleman (RSA) IKE keys.

  Workaround There is no workaround.

- CSCdy09595

  Symptoms A router may reload unexpectedly when it is booting up.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(11.8).

  Workaround There is no workaround.

- CSCdy27052

  Symptoms A router may reload unexpectedly.

  Conditions This symptom is observed on a Cisco 7500 router.

  Workaround There is no workaround.

- CSCdy35576

  Symptoms A Cisco AS5400 universal gateway may reload after memory resources are depleted.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(12) when H.323 calls are placed or received under stress conditions.

  Workaround There is no workaround.

- CSCin01252

  Symptoms A line protocol may flap on a router or the router may go down.

  Conditions This symptom is observed under high traffic conditions on a Cisco 7200 series router that is configured with a PA-T3, PA-E3, or PA-H port adapter, a Network Processing Engine (NPE-400), or a Network Service Engine-1 (NSE-1).

  Workaround Use dual interface versions of the port adapters mentioned above.

- CSCin03391

  Symptoms Pings cannot be sent between routers.

  Conditions This symptom is observed when a ping is sent from a customer edge (CE) router to another CE router via a provider edge (PE) router. This symptom occurs if the routers are configured using scripts.

  Workaround There is no workaround.

- CSCin04952

  Symptoms A router may reload after the **show voice call summary** EXEC command is issued.

  Conditions This symptom is observed on a Cisco 7200 router if the router is reloaded with a startup-config in which the same digital service zero (DS0) group number is associated with the same time slots more than once on a given controller. The following is an example of such an occurrence:

  ```
  ds0-group 0 timeslot 1 type e&m-winkstart
  ds0-group 0 timeslot 1 type e&m-winkstart
  ```

  Workaround Remove the redundant **ds0-group** controller configuration command from the startup-config. After reloading with the startup-config, issue the **write memory** command and reload the router.

- CSCin06016

  Symptoms A router may reload if a high density voice network module (NM-HDV) is brought up without a voice WAN interface card (VWIC).

  Conditions This symptom is observed on a Cisco 3660 router that has an NM-HDV. The router reloads if the router is started up without a VWIC, such as the 2-port T1 multiflex truck interface card with Drop and Insert (VWIC-2MFT-T1-DI).

  Workaround There is no workaround.

- CSCin06770

  Symptoms A BRI interface channel returns ifAdminStatus and ifOperStatus as down even when the channel is up and there is ongoing traffic.

Conditions This symptom is observed on the BRI 0:1 channel of a BRI interface on a Cisco 1700 router.

Workaround There is no workaround.

- CSCin06898

  Symptoms Static mapping does not get deleted.

  Conditions This symptom is observed on a multipoint ATM subinterface after a long time has elapsed. The static mapping does not get deleted even if the subinterface is in a shutdown condition.

  Workaround Delete the permanent virtual circuits (PVCs) on the multipoint ATM subinterface in order to delete the static mapping.

- CSCin07076

  Symptoms A router may reload after distributed Multilink PPP (dMLP) is enabled.

  Conditions This symptom is observed on a Cisco 7500 router after dMLP is enabled.

  Workaround There is no workaround.

- CSCin07457

  Symptoms A Kerberos SRVTAB entry on a router cannot be unconfigured and the following message may be displayed:

  ```
  Failed to remove srvtab entry!!!
  ```

  Conditions This symptom is observed on a Cisco router that has Kerberos configured.

  Workaround The SRVTAB entry can be removed by changing the *principal-type* argument in the **no kerberos srvtab entry** *kerberos-principal principal-type* to 0.

  Alternate Workaround If the NVRAM still contains the old SRVTAB entry, enter the **write erase** command and reload the router.

- CSCin08849

  Symptoms If the first dial peer routes and authorizes a call using the Open Settlement Protocol (OSP), subsequent attempts to set up the call with the rest of the dial peers on the list do not work.

  Conditions This symptom is observed when a dial peer rotary is used with OSP.

  Workaround There is no workaround.

- CSCin10067

  Symptoms When member links are removed from a multilink bundle (M2) and configured as members of another multilink bundle (M5), the M5 multilink bundle does not come up.

  Conditions This symptom is observed only with the distributed Multilink PPP (MLP) feature when a member link is reconfigured to be a member link of another multilink bundle. This symptom is observed only on Cisco 7500 series and Cisco 7600 series routers.

  Workaround There is no workaround.

- CSCin10071

  Symptoms A FlexWAN module may reload if the member link of a multilink bundle is removed by entering the **no channel-group** interface configuration command.

  Conditions This symptom is observed on a Cisco 7600 series router that has a FlexWAN module when distributed Multilink PPP (MLP) is configured.

Workaround Do not remove the member link using the no channel-group interface configuration command when the member link is in the UP state. Instead shut down the member link first, remove the multilink configuration for the member link, and remove the member link by entering the **no channel-group** interface configuration command.

- CSCin10568

  Symptoms Untagged entries appear in the Tag Forwarding Information Base (TFIB).

  Conditions This symptom is observed when you toggle a Label Distribution Protocol (LDP)/Tag Distribution Protocol (TDP) session by toggling the LDP router identification (ID). This situation occurs in Cisco IOS Release 12.0 (21.1)S2, Release 12.0(21.1)SY2, Release 12.2(8.4), Release 12.2(8.4)S, Release 12.2(8.5)T, or later versions of the above-mentioned releases.

  Workaround Enter the **clear ip route** *network* command to recover from the situation.

- CSCin11205

  Symptoms A router may reload when Frame Relay is configured on a serial interface before the Voice over Frame Relay (VoFR) dial peers are configured.

  Conditions This symptom is observed on a Cisco 7500 series router that has a serial interface.

  Workaround Configure at least one VoFR dial peer before configuring Frame Relay on the serial interface.

- CSCin11256

  Symptoms A Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) may reload when PPP over ATM (PPPoA) sessions are initiated.

  Conditions This symptom is observed when the **shutdown** interface configuration command and the **no shutdown** interface configuration command are entered in quick succession.

  Workaround There is no workaround.

- CSCin11716

  Symptoms A router does not complete a call using the next configured dial peer if the call does not go through with the first configured dial peer and the call is disconnected. This behavior is inconsistent with the expected behavior of the rotary dial peer feature.

  Conditions This symptom is observed on a Cisco router that has dial peers that are using the rotary dial peer feature and that are configured to perform settlement using the Open Settlement Protocol (OSP). This symptom is observed when more than one dial peer is configured with the same destination pattern. The rotary dial peer feature is configured on the dial peers using the **preference** *value* dial-peer configuration command. The first dial peer is configured with a preference value of 0, indicating that the dial peer would be the first dial peer to be selected when an inbound call is received.

  Workaround There is no workaround.

- CSCin11879

  Symptoms A router may reload when the **show policy interface** EXEC command is entered.

  Conditions This symptom is observed on a Cisco router if the policer is configured.

  Workaround There is no workaround.

- CSCin12742

  Symptoms The alarm indication signal (AIS) that is sent by a port adapter is not recognized. The AIS that is sent by the port adapter does not conform to existing standards.

Conditions This symptom is observed in a network in which two T3 multichannel port adapters (PA-MC-2T3) are configured in a back-to-back configuration for M23 framing.

Workaround There is no workaround.

- CSCin14598

  Symptoms A router may reload when a channel-associated signaling (CAS) is unconfigured on an E1 controller.

  Conditions This symptom is observed on an E1 controller on a Cisco 3640 router that has a digital modem network module (NM-DM).

  Workaround There is no workaround.

- CSCuk27655

  GRE implementation of Cisco IOS is compliant with RFC2784 and RFC2890 and backward compatible with RFC1701.

- CSCuk34118

  Symptoms If an online insertion and removal (OIR) is performed on a line card while a Cisco Express Forwarding (CEF) table is downloaded, the remaining line cards may pause indefinitely in the "request reload" state as they wait for the line card that has been installed using the OIR procedure to complete the download of the CEF table.

  Conditions This symptom is observed on a line card of a Cisco 12000 series Internet router.

  Workaround Reinstall the line card that has been installed using the OIR procedure into the out slot.

Novell IPX, XNS, and Apollo Domain

- CSCdv33639

  Symptoms On a router, the following message is displayed:

  ```
  %IPX-3-TOOMANYNETS: Too many networks
  ```

  Conditions This symptom is observed if the number of interfaces that are running the Internetwork Packet Exchange (IPX) protocol exceeds 200. This combination may include a variety of interfaces that are running the Routing Information Protocol (RIP), the Enhanced Interior Gateway Routing Protocol (EIGRP), or the NetWare Link Services Protocol (NLSP). However, if an interface is running both RIP and EIGRP simultaneously, it is considered to be running two protocols instead of one. This means that the 200 limit would be reached if there are 100 interfaces running both RIP and EIGRP.

  Workaround On an interface that is running both EIGRP and RIP, remove either one of the two protocols. Enter the **no network** *network-number* DHCP pool configuration command immediately after the **ipx router rip** global configuration command in the startup-config file of the router where the interface is installed.

- CSCdx16307

  Symptoms A router may display BADSHARE error messages such as the following:

  ```
  %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=60F59560, count=0 -Traceback=
  6030E63C 60767384 60767C48 60767D00 6071E434 60342374 60342360
  ```

  Conditions This symptom is observed when Internet Packet Exchange (IPX) compression is configured in the following way: **ipx compression cipx 100** on a Cisco 3620 router that is running Cisco IOS release 12.1(13).

  Workaround There is no workaround.

- CSCdx73624

  Symptoms Internetwork Packet Exchange (IPX) Service Advertisement Protocol (SAP) updates are not populated properly.

  Conditions This symptom is observed when both IPX Enhanced Interior Gateway Routing Protocol (EIGRP) and IPX Routing Information Protocol (RIP) are configured on a network.

  Workaround Disable the IPX RIP on the network.

TCP/IP Host-Mode Services

- CSCdw89700

  Symptoms When two Cisco routers are running data-link switching (DLSw) and are peered to the same 190 remote sites over a Frame Relay network through a High-Speed Serial Interface (HSSI), about 80 of the 190 DLSw peers disconnect and reconnect at irregular intervals.

  Some peers stay up for several hours, while others disconnect and reconnect frequently. The DLSw peers are disconnecting because the TCP stack has reached its retransmit threshold. When this condition occurs, extended pings (pings that are sourced by the IP address of the DLSw peer) to the IP address of the remote DLSw peer that is experiencing connectivity issues are consistently successful.

  During successive retransmission timeout, the timer receives a negative timeout value. This causes the packets to be on the retransmit queue for as long as KRTT even though they have been acked. If the **debug ip tcp** option is used and debug is turned on, the following error message is displayed when this problem occurs.

  ```
  "Received a negative sleep value:<value>"
  ```

  Conditions This symptom is observed in a configuration in which two Cisco 7507 routers are running Cisco IOS Release 12.1(13). Each Cisco 7507 router has a Channel Interface Processor 2 (CIP 2) that is connected to a mainframe. This symptom has also been observed on Cisco 3600 series, Cisco 7200 series, and Cisco 4700 series routers.

  Workaround There is no workaround.

- CSCdx22480

  Symptoms A signal trap (SIGTRAP) exception may cause a router to reload.

  Conditions This symptom is observed on a Cisco 2600 router that is running Cisco IOS Release 12.2(4)T3 and that is running X.25 protocol translation and X.25 routing. The router may restart unexpectedly if the **clear tcp tcb** *address* EXEC command is issued using a non-transmission control block (TCB) address.

  Workaround There is no workaround.

- CSCdx55357

  Symptoms TCP processing fails in the data repacketizing process and creates inaccurate packets. Symptoms may vary on the application using the TCP transport; a data-link switching (DLSw) circuit disconnects suddenly, and the following error message is displayed if you enter the **debug dlsw core** command on one for the DLSw routers:

  ```
  DLSW: Invalid dlsw version 78 (The number 78 is an example and may be any other
  number.)
  ```

  If the TCP session is a telnet session to the router, it may pause indefinitely, and the peer may indicate to receive packets with invalid TCP checksum.

Conditions These symptoms are observed when the sender side TCP peer is using Multilink PPP (MLP) for the outgoing link. These symptoms are observed during an attempted TCP retransmission of a message after multiple consecutive TCP packets have been lost (for example, due to a network outage or policing somewhere in the interconnecting network), and TCP data packet reconstruction. These symptoms are observed only with a TCP session directly terminated on this sender side TCP peer, not with any traffic passed through the router.

Workaround: Disable MLP on the outbound interface.

Wide-Area Networking

- CSCdu48304

  Symptoms Frame Relay Forum compression (FRF.9) is not negotiated when keepalives are disabled.

  Conditions This symptom is observed if the Frame Relay configuration is added after an interface is shut down (by entering the **shutdown** interface configuration command) and before the **no shutdown** interface configuration command is entered on the interface.

  Workaround Wait a few seconds before entering the **no shutdown** interface configuration command on the interface.

- CSCdv68371

  Symptoms The first one or two calls may fail.

  Conditions This symptom is observed when calls are made through two Cisco 3640 routers that are running Cisco IOS Release 12.2(5.3)T or Release 12.2(5.4) through an E1 PRI interface card that is configured on High Density Voice (HDV) ports.

  Workaround There is no workaround.

- CSCdw52143

  Symptoms The values of the ifHCInOctets and ifHCOutOctets MIB objects show an abnormally high rate of increase.

  Conditions This symptom is observed on emulated network interfaces that correspond to LAN Emulation (LANE) clients. The rate of increase of the ifHCInOctets and ifHCOutOctets MIB objects is much higher than the maximum possible rate of the ifHighSpeed values for the interface.

  Workaround There is no workaround.

- CSCdw56848

  Symptoms A router may reload because of a bus error or a software-forced reload.

  Conditions This symptom is observed on a Cisco 3640 router that is running Cisco IOS Release 12.2(3) or Release 12.2(6). When this symptom occurs, call tracker processes are present in the stack trace even though call tracker is not supported nor configured on the Cisco 3640.

  Workaround There is no workaround.

- CSCdw62563

  Symptoms A router may fail to place an outgoing call and may display the “no bundle in dialer_fsm_up” message.

  Conditions This symptom is observed on a router that has a dialer profile configuration.

  Workaround There is no workaround.

- CSCdw71398

  Symptoms Active calls may be dropped if the D channel is enabled or disabled.

  Conditions This symptom is observed on the serial interface of a Signaling System 7 (SS7) Interconnect Solution when the interface is shut down. When this condition occurs, Layer 2 is not brought down immediately and active calls will be dropped if the D channel is enabled or disabled.

  Workaround There is no workaround.

- CSCdx00073

  Symptoms A call comes in from a PRI with an empty asynchronous network interface (ANI) information element (IE) in the ISDN setup message but the router sends an outgoing ISDN message that does not have an ANI IE.

  Conditions This symptom is observed on a Cisco 2600 router that is running Cisco IOS Release 12.2(7a).

  Workaround There is no workaround.

- CSCdx00311

  Symptoms The Layer 2 Tunneling Protocol (L2TP) network server (LNS) reloads after the L2TP access concentrator (LAC) sends a Call Disconnect Notification (CDN).

  Conditions This symptom is observed on an LNS that is configured to call back the dial-in user when the string that is sent by the LNS during a callback is the correct string, but the LAC uses a different string to dial out.

  Workaround There is no workaround.

- CSCdx04773

  Symptoms Calls that have unsupported traffic parameters are released when a Cisco router is running User-to-Network Interface (UNI) version 4.0 software with a vendor-specific switch.

  Conditions This symptom is observed if a Cisco router is connected to a vendor-specific switch and if the router is configured to operate UNI version 4.0 software across the unnegotiated router-switch link. The calls are released by the Cisco router if any traffic parameter is modified on the unnegotiated link.

  Workaround Use UNI version 3.1.

- CSCdx12421

  Symptoms When the name information is sent on a vendor-specific switch using a display information element (IE), the first character of the name may be stripped. For example, “John Smith” may be displayed as “ohn Smith.”

  Conditions This symptom is observed if both the vendor-specific switch and the router are configured with the Digital Multiplex System (DMS 100) protocol. This symptom is observed if the router does not send the first octet of the display IE as 0xB1 (which is part of the DMS 100 protocol).

  Workaround Insert a space before the first character of the name information display on the system that originates the call. Alternately, the ISDN circuit that is connected to the vendor-specific switch can be configured so that it is controlled by the Cisco Call Manager.

- CSCdx12555

  Symptoms Memory fragmentation with MALLOCFAIL messages in the pool processor may occur on a router.

Conditions This symptom is observed on a Cisco 7206 router with a Network Processing Engine (NPE-200) that is running Cisco IOS Release 12.1(9.05).

Workaround There is no workaround.

- CSCdx13821

  Symptoms The dialer redial interface configuration command may not work as expected with caller ID callback.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(7a). The router detects active channels after the channels have been cleared and after the **dialer redial** interface configuration command has been issued on the router. The presence of active channels can be verified by issuing the **show isdn active** EXEC command or the **show isdn service** EXEC command on the router.

  Workaround Remove the **dialer redial** interface configuration command from the configuration.

- CSCdx18069

  Symptoms A memory leak of 80 Kb per minute may occur with the ISDN process, and the following messages may be displayed:

  ```
  %AMDP2_FE-5-LATECOLL: FastEthernet0/0 transmit error
  %ISDN-6-LAYER2DOWN: Layer 2 for Interface Se7/0:15 SC, TEI 0 changed to down
  %ISDN-4-RLM_STATUS_CHANGE: ISDN SC Se7/0:15 SC: Status Changed to: Link Up.
  %ISDN-6-LAYER2UP: Layer 2 for Interface Se7/0:15 SC, TEI 0 changed to up
  ```

  Conditions This symptom is observed when Signaling System 7 (SS7) bulk calls are made through an H.323 medium and occurs after the Fast Ethernet interface exhibits transmission difficulty and causes the Redundant Link Manager (RLM) to bounce.

  Workaround There is no workaround.

- CSCdx19655

  Symptoms A router may reload at the fr_frag_turbo_capable process when Frame Relay encapsulation is unconfigured prior unconfiguring features.

  Conditions This symptom is observed on a Cisco 7200 router that is running the c7200-js-mz.122-8.T1 image of Cisco IOS Release 12.2(8)T1.

  Workaround There is no workaround.

- CSCdx22533

  Symptoms ISDN may send an incorrect release cause code for a normal Signaling System 7 (SS7) call. ISDN receives a valid cause information element (0xC284) in a disconnect message, but it releases the “cause=invalid information element contents” cause code. The following is a sample of the incorrect release cause code:

  ```
  ISDN Se7/7:0 SC Q931: RX <- DISCONNECT pd = 8  callref = 0x0017
  Cause i = 0xC284 - Vacant code or prefix digit not dialed
  ISDN Se7/7:0 SC Q931: TX -> RELEASE pd = 8  callref = 0x8017
  Cause i = 0x80E4 - Invalid information element contents
  ```

  Conditions This symptom is observed on a Cisco AS5400 universal access server that is handling SS7 calls.

  Workaround There is no workaround.

- CSCdx23472

  Symptoms Inbound overlap calls to a router may fail.

Conditions This symptom is observed on a Cisco 2600 router that is configured for BRI Q-signaling (QSIG) and overlap receiving. This symptom occurs only if ISDN SHORT-CALL-REFERENCE is configured on the BRI interface. The inbound overlap calls will work if there is an exact matching dial peer.

Workaround Ensure that there is an exact matching dial peer for inbound overlap calls.

- CSCdx23889

  Symptoms Calls may be rejected when a gateway performs overlap sending such as in calls in which the called party number exceeds 20 digits.

  Conditions This symptom is observed on a gateway when the gateway uses overlap sending. The gateway rejects the call if a call proceeding message is received without a channel identity (ID) even though a channel ID has already been received in a setup acknowledgement message and a channel ID is not required.

  Workaround There is no workaround.

- CSCdx24399

  Symptoms After a virtual interface comes up, the first few packets are process switched or fast switched instead of being switched by Cisco Express Forwarding (CEF). CEF switching may resume after a minute.

  Conditions This symptom occurs when CEF is used on virtual access interfaces (such as virtual profiles, virtual private dial-up networks (VPDNs), and Multilink PPP [MLP]).

  Workaround There is no workaround.

- CSCdx24569

  Symptoms An incorrect call state may be indicated in a Q.931 setup message.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(2)XB03 when a call is placed on a phone that is connected to the router through a Foreign Exchange Station (FXS).

  Workaround There is no workaround.

- CSCdx25923

  Symptoms A Frame Relay over ISDN call is not retried after it is dropped.

  Conditions This symptom occurs when Frame Relay over ISDN is used. If a data-link connection identifier (DLCI) that is configured on a subinterface goes down (becomes inactive or is deleted), the corresponding subinterface is marked down. When the ISDN circuit is released, the subinterface remains in the down state. Subsequent attempts to bring up the ISDN circuit using the network address that is bound to that subinterface do not work.

  Workaround Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the subinterface.

- CSCdx28734

  Symptoms A network side router may disconnect a call and display the “Cause i = 0x8286 - Channel unacceptable” cause code.

  Conditions This symptom is observed on a Cisco 3640 router that has a high density voice network module (NM-HDV) and a BRI voice interface card (VIC) and that is running Cisco IOS Release 12.2.

  Workaround There is no workaround.

- CSCdx28814

  Symptoms A router with Frame Relay switched virtual circuits (SVCs) may fail to pass IP traffic on those SVCs. The following message is displayed: %PVC already assigned to sub-interface Serial 1.2

  Conditions This symptom is observed on a Cisco 4000 series router that is running Cisco IOS Release 12.0(7)T and on a Cisco 2600 router that is running Cisco IOS Release 12.2(6). The router has configured two Frame Relay SCVs on a single physical interface. At the first attempt both SVCs are established. However, if you wait for one SCV to time out and then try to establish the second one, the symptom will occur. the 2600 platform for the This has been found in 12.0(7)T for the 4000 series and 12.2(6) on the 2600 platform. Suspect that this affects all versions of IOS and is platform independent.

  The initial SVC call may come active and pass traffic. However, if the call gets disconnected and another call is generated with the same data-link connection identifier (DLCI) assigned by the switch, the DLCI will still show as active in a **show frame-relay** permanent virtual circuit (PVC) command and will still be assigned to the original interface or subinterface.

  If a second call is made to the same IP address and the same DLCI, the call will succeed. If this second call is to a different IP address (a different subinterface), the call will fail.

  The **show frame-relay** map command will show the IP address to virtual circuit (VC) mapping removed after the initial call is cleared. However, the **show frame-relay** PVC command will still show that the DLCI as active.

  Workaround There is no workaround.

- CSCdx37937

  Symptoms Advice of charge (AOC) ISDN messages are terminated on a voice-enabled gateway.

  Conditions This symptom is observed on a Cisco gateway that has voice enabled and that is running Cisco IOS Release 12.2(6a).

  Workaround There is no workaround.

- CSCdx47905

  Symptoms A router may reload if PRI group time slots are partially unconfigured. The entire PRI group configuration is removed from the controller if the **no pri-group** controller configuration command is issued.

  Conditions These symptoms are observed on a Cisco router after the **no pri-group** controller configuration command is issued. Currently ISDN does not support partial unconfiguration of a PRI group.

  Workaround There is no workaround.

- CSCdx54104

  Symptoms A Cisco 3640 router cannot keep both B channels up at the same time. An increase in the traffic load causes the second B channel to connect after the first one drops. The B channels are in the up state alternately, but the B channels are never up at the same time.

  Conditions This symptom is observed on a Cisco 3640 router that is running Cisco IOS Release 12.2(2).

  Workaround There is no workaround to keep both channels up. However, one B channel can be kept in the up state by increasing the value of the load argument in the **dialer load-threshold** *load* interface configuration command to 255.

- CSCdx55880

  Symptoms Up/Down status messages are displayed on the console.

Conditions This symptom is observed when PPP calls the interface reset vector while the Link Control Protocol (LCP) is configured or closes. If a leased- line configuration is up but the peer is not responding, PPP may call the interface reset vector approximately once per minute. This situation may result in Up/Down status messages on the console.

This DDTS adds the new **no ppp link reset** command to disable calls to the interface reset vector. PPP will continue to attempt to negotiate with the peer, but the interface will not be reset between each attempt.

Workaround There is no workaround.

- CSCdx56539

  Symptoms Outgoing V.110 calls that are made to some terminal adapters (TAs) fail on BRI interfaces that have Modem ISDN channel aggregation (MICA) technologies modems.

  Conditions This symptom is observed on a Cisco router that has MICA modems installed on BRI interfaces.

  Workaround There is no workaround.

- CSCdx62798

  Symptoms A router may reload because of an ISDN memory leak.

  Conditions This symptom is observed when Signaling System 7 (SS7) calls are made between an originating and a terminating gateway. The symptom is observed when the underlying physical layer is unstable. This may include instances when Layer 2 and Layer 3 bounce at regular intervals. This memory leak does not occur under normal SS7 working conditions when Layers 2 and 3 are stable.

  Workaround There is no workaround.

- CSCdx63820

  Symptoms An intercom call on a Cisco router is cleared after an incoming call is received on either one of the two ports that are engaged in the intercom call.

  Conditions This symptom is observed on a Cisco 800 series router when an incoming call is received on either port 1 or port 2 while both of the ports are engaged in an intercom call.

  Workaround There is no workaround.

- CSCdx67897

  Symptoms BRI calls that are of the +ts013 switch type are disconnected by a remote peer.

  Conditions This symptom is observed on a Cisco 4224 router that is running Cisco IOS Release 12.2.

  Workaround There is no workaround.

- CSCdx72556

  Symptoms Link Control Protocol (LCP) negotiations may fail, and a “failed to negotiate with peer” message may be displayed.

  Conditions This symptom is observed on a Cisco universal access server if the peer sends more than five Configure-Negative acknowledgments (CONFNAKs) or Configure-Rejects (CONFREJs) on the link for the current or previous LCP negotiation.

  Workaround Configure the **ppp max-failure 10** command on the link to allow the remote peer to exhaust the Negative acknowledgment (NAK) or Reject acknowledgment (REJ) count and resume negotiations before the Cisco universal access server drops the link.

- CSCdx74747

  Symptoms Spurious memory accesses may be observed on a router.

Conditions This symptom is observed on a Cisco 7200VXR router.

Workaround There is no workaround.

- CSCdx77219

  Symptoms A router may terminate outgoing ISDN calls with an "i = 0x80AF - resource unavailable, unspecified" cause code. The following error message may be displayed if this symptom occurs because there is no dial tone for about 15 minutes:

  ```
  %ISDN-6-CALL_COLLISION: Interface Se1/0:15 Call Cid 0xD8C Cref 0x800D collision on
  Channel 1 in_use_cid 0xD8B cref 0x800C, Channel awarded to the received call
  ```

  Conditions This symptom is observed on a Cisco 3640 router that is running Cisco IOS Release 12.2(10a).

  Workaround There is no workaround.

- CSCdx77748

  Symptoms A data terminal ready (DTR) dialer may not work with High-Level Data Link Control (HDLC) encapsulated packets.

  Conditions This symptom is observed on a DTR dialer. This symptom does not affect PPP encapsulated packets.

  Workaround There is no workaround.

- CSCdx77888

  Symptoms Input Multiprotocol Label Switching (MPLS) packets are not accounted for by permanent virtual circuits (PVCs) that are configured on a Versatile Interface Processor (VIP) interface. The input counters in the output of the show frame-relay pvc EXEC command are not updated.

  Conditions This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.2.

  Workaround There is no workaround.

- CSCdx80488

  Symptoms The **frame-relay intf-type dce** interface configuration command cannot be configured on a dialer interface.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(11.2).

  Workaround There is no workaround.

- CSCdx84284

  Symptoms A router may not recognize some inbound Multiprotocol Label Switching (MPLS)-tagged packets that are sent via Frame Relay. Because the router cannot recognize the inbound MPLS-tagged packets, MPLS cannot switch those packets to the outgoing interface. The MPLS-tagged packets are dropped by the router, and the router does not increment the input-packet counter in the output of the **show frame pvc** output EXEC command.

  Conditions This symptom is observed on a Cisco router that has Cisco Express Forwarding (CEF) enabled and that is running Cisco IOS Release 12.2(7b).

  Workaround Enable the **debug mpls packets** EXEC command.

- CSCdx89160

  Symptoms Under rare circumstances, a software-forced reload may be observed on a Cisco AS5850 universal gateway when the **redundancy handover peer busy-period n** privileged EXEC command is entered.

  Conditions This symptom is observed on a Cisco AS5850 universal gateway that is operating in the handover split mode in a Signaling System 7 (SS7) solution.

  Workaround There is no workaround.

- CSCdy18949

  Symptoms An ISDN BRI interface does not use the T302 timer as an interdigit timer.

  Conditions This symptom is observed only with voice calls on an ISDN BRI interface that is configured for overlap receiving on a Cisco router that is running Cisco IOS Release 12.2(6e). This symptom does not affect modem or data calls. The inbound dial peer for the voice call does not have the **direct-inward-dial string** dial-peer configuration command configured.

  Workaround There is no workaround.

- CSCdy23678

  Symptoms After a TCP connection is terminated, the TCP transmissions that are sent by a router are corrupted. The last 6 bytes of the IP header are duplicated in the packet and appear as the first 6 bytes of the TCP header.

  Conditions This symptom is observed on the outgoing interface of a Cisco router that is running Multilink PPP (MLP).

  Workaround Disable MLP.

- CSCdy24524

  Symptoms A router may reload if the **isdn leased-line** global configuration command is configured on a BRI interface that is in the shutdown state.

  Conditions This symptom is observed of a BRI interface on a Cisco router.

  Workaround Do not put the BRI interface into the shutdown state before the **isdn leased-line** global configuration command is configured.

- CSCin04769

  Symptoms A universal access sever may reload while it attempts to call another universal access server.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that is running the c5300-js-mz.122-2.XB image of Cisco IOS Release 12.2(2)XB. This symptom occurs when the Cisco AS5300 initiates a V.110 call to a Cisco 5850 universal access server.

  Workaround There is no workaround.

- CSCin07771

  Symptoms A universal access server may reload with a bus error at the dsx1_init_pri process.

  Conditions This symptom is observed on a Cisco AS5300 universal access server after ISDN Non-Facility Associated Signaling (NFAS) is configured.

  Workaround Configure the primary NFAS interface before configuring other NFAS members in the group.

- CSCuk33657

  Symptoms A traceback error message regarding illegal memory reference may be displayed.

Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(10.1) or Release 12.2(10.1)T after Frame Relay traffic shaping is configured.

Workaround There is no workaround.

- CSCuk36585

  Symptoms A gateway that has an ISDN PRI interface does not use T301 as an interdigit timer.

  Conditions This symptom is observed on a Cisco gateway that is running Cisco IOS Release 12.2(6g) and that has an ISDN PRI interface that is configured for overlap receiving.

  Workaround There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(10g)

Cisco IOS Release 12.2(10g) is a rebuild release for Cisco IOS Release 12.2(10). The caveats in this section are resolved in Cisco IOS Release 12.2(10g) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

Symptoms—A description of what is observed when the caveat occurs.

Conditions—The conditions under which the caveat has been known to occur.

Workaround—Solutions, if available, to counteract the caveat.

IP Routing Protocols

- CSCdx40184

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCed28873

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

Miscellaneous

- CSCdx76632

  Symptoms: A Cisco AS5300 that is functioning as a voice gateway may reload because of an incoming bus error exception.

  Conditions: This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(6d).

  Workaround: There is no workaround.

- CSCdx77253

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea19885

  Symptoms: A Cisco router that has a voice feature such as H.323 enabled may reload because of a bus error at address 0xD0D0D0B.

  Conditions: This symptom is observed on a Cisco 3700 series but may also occur on other routers.

  Workaround: There is no workaround.

- CSCea32240

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea33065

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea36231

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea46342

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51030

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51076

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea54851

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCeb78836

  Symptoms: Cisco IOS software may cause a Cisco router to reload unexpectedly when the router receives a malformed H.225 setup message.

  Conditions: This symptom is observed on a Cisco 1700 series that runs Cisco IOS Release 12.2(13c). The symptom occurs when the following **debug** privileged EXEC commands are enabled:

  - **debug h225 asn1**
  - **debug h225 events**
  - debug h225 q931

  Workaround: There is no workaround.

- CSCec86420

  Symptoms: When you enter the **undebug all** privileged EXEC command on a Cisco 3700 series, all traffic that passes through an encrypted generic routing encapsulation (GRE) tunnel may stop.

  Conditions: This symptom is observed on a Cisco 3700 series that is configured with a GRE tunnel that is secured via IP Security (IPSec) and that is using Cisco Express Forwarding (CEF) switching.

Workaround: Reinitialize CEF switching by entering the **no ip cef** global configuration command followed by the **ip cef** global configuration command.

- 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.

- CSCin56408

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at

http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

Resolved Caveats—Cisco IOS Release 12.2(10d)

Cisco IOS Release 12.2(10d) is a rebuild release for Cisco IOS Release 12.2(10). The caveats in this section are resolved in Cisco IOS Release 12.2(10d) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

Symptoms—A description of what is observed when the caveat occurs.

Conditions—The conditions under which the caveat has been known to occur.

Workaround—Solutions, if available, to counteract the caveat.

Basic System Services

- CSCdy46150

  Symptoms: A Cisco 7206VXR router may experience memory allocation (malloc) failures.

  Conditions: This symptom occurs when a Cisco 7206VXRrouter with a Network Processing Engine (NPE-400) has 256 MB of memory but only has 16 MB of I/O memory configured.

  Workaround: There is no workaround. Use the **memory-size** iomen global configuration command to configure more I/O memory.

Miscellaneous

- 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.

- CSCdx76632

  Symptoms: A Cisco AS5300 that is functioning as a voice gateway may reload because of an incoming bus error exception.

  Conditions: This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(6d).

  Workaround: There is no workaround.

- CSCdx77253

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCdz16414

  Symptoms: Network Time Protocol (NTP) may not remain synchronized.

  Conditions: This symptom is observed on a Cisco ONS 15104. After several minutes of operation, the clock wanders and the NTP becomes unsynchronized.

  Temporary Workaround: Deconfigure and reconfigure the NTP configuration to enable the NTP to synchronize again until the symptom reoccurs.

- CSCdz71127

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

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

  This advisory is available at

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

- CSCea02355

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

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

  This advisory is available at

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

- 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.

- CSCea32240

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea33065

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea36231

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at
  http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea46342

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51030

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea51076

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

- CSCea54851

  Cisco products running IOS contain vulnerabilities in the processing of H.323 messages, which are typically used in packetized voice or multimedia applications. Features such as NAT and IOS Firewall must inspect H.323 messages and may be vulnerable as well. A test suite has been developed by the University of Oulu to target this protocol and identify vulnerabilities.

  Support for the H.323 protocol was introduced in Cisco IOS Software Release 11.3T, and all later Cisco IOS releases are affected if configured for various types of Voice/Multimedia Application support. The vulnerabilities can be exploited repeatedly to produce a denial of service (DoS).

  There are workarounds available that may mitigate the impact, but these techniques may not be appropriate for use in all customer networks.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml.

Resolved Caveats—Cisco IOS Release 12.2(10b)

Cisco IOS Release 12.2(10b) is a rebuild release for Cisco IOS Release 12.2(10). The caveats in this section are resolved in Cisco IOS Release 12.2(10b) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

Symptoms—A description of what is observed when the caveat occurs.

Conditions—The conditions under which the caveat has been known to occur.

Workaround—Solutions, if available, to counteract the caveat.

- CSCdx69505

  Symptoms A Cisco router incorrectly resets the Logical Link Control, type 2 (LLC2) retransmission count to zero.

  After a Cisco router has sent an information frame (I-frame), it will wait for an acknowledgement. If the LLC2 T1 timer expires before this acknowledgment is received, the router retransmits the I-frame and increments the LLC2 transmission count. The router resets the transmission count when it receives an LLC2 frame that has the final bit turned on. However, the router should reset the retransmission count when it receives an LLC2 frame that acknowledges outstanding I-frames.

  Conditions The symptoms occur only rarely.

  Workaround There is no workaround.

- CSCdw89700

  Symptoms When two Cisco 7507 routers are running data-link switching (DLSw) and are peered to the same 190 remote sites over a Frame Relay network through a High-Speed Serial Interface (HSSI), about 80 of the 190 DLSw peers disconnect and reconnect at irregular intervals.

  Some peers stay up for several hours, while others disconnect and reconnect frequently. The DLSw peers are disconnecting because the TCP stack has reached its retransmit threshold. When this condition occurs, extended pings (pings that are sourced by the IP address of the DLSw peer) to the IP address of the remote DLSw peer that is experiencing connectivity issues are consistently successful.

  Conditions This symptom is observed in a configuration in which two Cisco 7507 routers are running Cisco IOS Release 12.1(13). Each Cisco 7507 router has a Channel Interface Processor 2 (CIP 2) that is connected to a mainframe.

  Workaround There is no workaround.

- CSCdx25471

  Symptoms A Cisco AS5800 router shelf (RS) reloads after a Service Processing Element (SPE) module has reloaded.

  Conditions This symptom is observed on a Cisco AS5800 that is configured with a Universal Port Card using NextPort software.

  Workaround There is no workaround.

- CSCdv34579

  Symptoms A Versatile Interface Processor (VIP), Gigabit Ethernet Interface Processor (GEIP), Gigabit Ethernet Interface Processor plus (GEIP+), or Packet OC-3 Interface Processor (POSIP) that is installed in a router may reload. The VIP may display the following error message when it reloads:

  ```
  %DMA-1-DRQ_STALLED: DRQ stalled. Dumping DRQ.
  ```

  Conditions This symptom is observed on a Cisco 7500 series router under heavy traffic conditions.

Workaround There is no workaround.

- CSCdx57538

  Symptoms IP security (IPSec) traffic occurs intermittently over an IPSec generic routing encapsulation (GRE) tunnel.

  Conditions This symptom is observed when you use a hardware encryption card in Cisco IOS Release 12.2(7a) or Release 12.2(7b). The IPSec GRE tunnel itself works fine.

  Workaround There is no workaround.

- CSCdv40244

  Symptoms The following continuous stream of "%POT1E1-3-FWFATAL" error messages may occur on a router:

  ```
  %POT1E1-3-FWFATAL: Bay 5: firmware needsresetdue to fw watchdog timeout
  %POT1E1-3-FWFATAL: Bay 4: firmware needsresetdue to fatal softwareerrors
  ```

  Conditions This symptom is observed on a Cisco 7206VXR router that is running Cisco IOS Release 12.1(8.04) and that is configured with a PA-MC-8T1 port adapter, but may also affect the PA-MC-2T1, PA-MC-4T1, PA-MC-8DSX1, PA-MC-2E1/120, and PA-MC-8E1/120 port adapters.

  Workaround There is no workaround.

- CSCdx26997

  Symptoms After an ISDN link is up, a Virtual Private Network (VPN) module drops packets from the ISDN link.

  Conditions This symptom is observed on a VPN module that is installed in a Cisco 2600 series or Cisco 3600 series router that is running Cisco IOS Release 12.2(7a) or a later release when hardware encryption is used. The symptoms do not occur when software encryption is used.

  Workaround Configure the **no ppp multilink fragmentation** command on the dialer interface.

- CSCdx55357

  Symptoms TCP processing fails in the data repacketized process and creates inaccurate packets. A data-link switching (DLSw) circuit disconnects suddenly, and the following error message is displayed if you enter the **debug dlsw core** command on one for the DLSw routers:

  ```
  DLSW: Invalid dlsw version 78
  ```

  The number 78 is an example and may be any other number.

  Conditions These symptoms are observed when the sender side TCP peer is using Multilink PPP (MLP) for the outgoing link. These symptoms are observed during an attempted TCP retransmission of a message and TCP data packet reconstruction on a DLSw router.

  Workaround Disable MLP on the outbound interface.

- CSCdx82069

  Symptoms A Cisco AS5400HPX cannot be booted with any image. The following messages appear on the console.

  ```
  rommon 3 > boot
  bus error while trying to access flash - addr = 0xb8000000
  cannot read flash info
  getdevnum warning: device "boot flash" has size of zero
  bus error while trying to access flash - addr = 0xb8000000
  cannot read flash info
  getdevnum warning: device "boot flash" has size of zero
  open: read error...requested 0x4 bytes, got 0x0
  trouble reading device magic number
  ```

```
boot: cannot open "bootflash:"
boot: cannot determine first file name on device "bootflash:"
rommon 4 >
```

Conditions These symptoms are observed on a Cisco AS5400HPX that is running Cisco IOS Release 12.2(7.4) or a later 12.2 release.

Workaround There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(10a)

Cisco IOS Release 12.2(10a) is a rebuild release for Cisco IOS Release 12.2(10). The caveats in this section are resolved in Cisco IOS Release 12.2(10a) but may be open in previous Cisco IOS releases.

The following information is provided for each caveat:

Symptoms—A description of what is observed when the caveat occurs.

Conditions—The conditions under which the caveat has been known to occur.

Workaround—Solutions, if available, to counteract the caveat.

- CSCdw27216

  Symptoms Several "RX FIFO was stuck - forced to reset MAC" messages may be logged on the console of a router. This message is specific to port adapters and I/O cards that use a vendor-specific chipset.

  Conditions This symptom is observed on a Cisco 7200 router that is operating in the normal mode. The following is a list of the affected port adapters and I/O cards:

  - 2-port Fast Ethernet 100BASE-TX port adapter (PA-2FE-TX)
  - 2-port Fast Ethernet 100BASE-FX (PA-2FE-FX)
  - Cisco 7200 I/O controller with 2 Fast Ethernet ports (C7200-I/O-2FE/E)
  - Cisco 7200 I/O controller with 2 Gigabit Ethernet ports (C7200-I/O-GE+E)

  Workaround There is no workaround.

- CSCdw41145

  Symptoms When a rotary dial peer is used with the Debit Card 2.0.0 Tool Command Language (TCL), only the first and the last missed rotary attempts are sent to the RADIUS server.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that is running Cisco IOS Release 12.2. This symptom occurs if more than two dial peers are tried in order to reach a destination when the Debit Card feature is used (with each dial peer set to use different priorities). This symptom occurs only if the **aaa accounting connection h323 start-stop radius** global configuration command is configured.

  Workaround There is no workaround.

- CSCdw70296

  Symptoms If policing is the only feature that is configured under a class map, the packets that are classified into this class map are also queued under the same class even though the packets should actually be queued under the class-default class map.

  Conditions This symptom is observed on a router that is running Cisco IOS Release 12.2. This symptom may cause packet reordering issues when policing is used to set some fields in the packet.

  Workaround There is no workaround.

- CSCdw95464

  Symptoms A universal access server may reload because of a bus error when analog calls are made.

  Conditions This symptom is observed on a Cisco AS5800 universal access server that is running Cisco IOS Release 12.2(2)XB05.

  Workaround There is no workaround.

- CSCdx10820

  Symptoms A router may reload with a bus error.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(7.4).

  Workaround There is no workaround.

- CSCdx11366

  Symptoms The maximum number of modular quality of service (MQC) command-line interface policy maps on a router is limited to 256.

  Conditions This symptom is observed on a Cisco 7200 router that is running Cisco IOS Release 12.2(8)T. CSCdv64193 imposed the restriction on the maximum number of policy maps that can be issued on a router to 256.

  Workaround Use Cisco IOS Release 12.2 T or Release 12.2(8)T1. In Cisco IOS Release 12.2(8)T1 and Release 12.2 T, the maximum number of policy maps that can be configured on a platform is based on what a given platform can support.

- CSCdx14794

  Symptoms A modem call does not send data after the data send ready (DSR) signal comes up on the modem.

  Conditions This symptom is observed on a Cisco AS5800 universal access server that has a Cisco AS5800 series 324-port card that has a Cisco NextPort modem. The client side may keep sending PPP and Link Control Protocol (LCP) frames until a timeout occurs.

  Workaround There is no workaround.

- CSCdx28239

  Symptoms A gateway may incorrectly fail Q Signaling (QSIG) passthrough or signaling-only calls.

  Conditions This symptom is observed on a Cisco gateway that is running Cisco IOS Release 12.2(7a) and that is used with a gatekeeper to perform zone bandwidth management. When a gatekeeper is used to perform zone bandwidth management, a Registration, Admission, and Status Protocol (RAS) admission request (ARQ) message is sent to the gatekeeper to resolve the destination and reserve bandwidth for the bearer channels. QSIG passthrough or signaling-only messages do not open bearer channels and do not use any bandwidth, but the generated ARQ message may erroneously reserve bandwidth. If the managed link has no more bandwidth available, the QSIG passthrough messages are rejected when they should actually be accepted. Because of this behavior, QSIG passthrough tunneling cannot occur if the link is saturated.

  Workaround There is no workaround.

- CSCdx32133

  Symptoms A router may reload with a bus error at address 0x500.

  Conditions This symptom is observed on a Cisco 7500 router that has a Route Switch Processor (RSP4) and that is running Cisco IOS Release 12.2(9.4a).

  Workaround There is no workaround.

- CSCdx32947

  Symptoms When the **ip pim rp-address** *ip-address* [*group-access-list*] [**override**] [*bidir*] global configuration command is configured, a conflict that is learned from an Auto Rendezvous Point (Auto-RP) announcement is still used even if the **override** keyword is specified.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2 S. The router will still accept information from the Auto-RP when this symptom occurs. This symptom will not occur if routers do not have conflicting information.

  Workaround There is no workaround.

- CSCdx37171

  Symptoms A router sends T-protocol data units (T-PDUs) to the incorrect User Datagram Protocol (UDP) port.

  Conditions This symptom is observed on a Cisco General Packet Radio Service (GPRS) support node (GGSN) that is running Cisco IOS Release 12.2(8.4). This symptom occurs if two different serving GPRS support nodes (SGSNs) are included for data and signaling in the create request.

  Workaround There is no workaround.

- CSCuk27655

  GRE implementation of Cisco IOS is compliant with RFC2784 and RFC2890 and backward compatible with RFC1701.

Resolved Caveats—Cisco IOS Release 12.2(10)

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(10). All the caveats listed in this section are resolved in Cisco IOS Release 12.2(10). This section describes severity 1 and 2 caveats and select severity 3 caveats.

The following information is provided for each caveat:

- **Symptoms**—A description of what is observed when the caveat occurs.
- **Conditions**—The conditions under which the caveat has been known to occur.
- **Workaround**—Solutions, if available, to counteract the caveat.

Access Server

- CSCdt05760

  Symptoms A Cisco AS5300 may return the following error when the **show modem operational-status** [*slot*/*port*] privileged EXEC command is entered:

  ```
  Modem slot/port already had OOBP command under execution, please try later
  ```

  This symptom affects all modems on a carrier card.

  Conditions This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.1(9) or an earlier release.

  Workaround There is no workaround.

- CSCdu31070

  Symptoms Connection times for incoming V.110 calls may vary because of an occasional loss of the first Link Control Protocol (LCP) CONFREG frame from the global system for mobile communication (GSM) set.

  Calls exhibiting this loss take approximately 2 seconds longer to connect than normal calls.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdv08170

  Symptoms "DS-RS flow control has got out of sync" messages be displayed when analog calls are cleared using the **clear spe** EXEC command. This condition may impact service on an access server.

  Conditions This symptom is observed on a fully loaded Cisco AS5800.

  Workaround There is no workaround.

- CSCdw44612

  Symptoms Stray or false outgoing calls may be placed on a Cisco AS5800

  Conditions This symptom is observed under rare circumstances and may occur even when the lines are configured for dial-in only.

  Workaround There is no workaround.

Basic System Services

- CSCdt81722

  A Cisco 7500 series router that is running Cisco IOS Release 12.1(7) and that is configured for Frame Relay switching over an IP generic routing encapsulation (GRE) tunnel passes data only in one direction. This situation occurs when a multichannel T1 card (for example, an eight-port multichannel T1 port adapter (PA-MC-8T1) or a PA-MC-4T1 port adapter) is installed in a Versatile Interface Processor (VIP) and the serial interface associated with the T1 controller port is configured to route an incoming data-link connection identifier (DLCI) to a tunnel interface. The permanent virtual circuits appear active, but IP fails across the tunnel.

  Workaround: Use a Fast Serial Interface Processor (FSIP) with an external CSU instead of the PA-MC-8T1 or PA-MC-4T1 port adapter.

- CSCdv18617

  When the **rotary-group** number configuration command is entered on asynchronous lines in Cisco IOS Release 12.2(3), the command brings on the effect of the **rotary** *group* [**queued**] line configuration command. For more information on how the **rotary** *group* [**queued**] line configuration command, refer to the chapter on Asynchronous Rotary Line Queueing at the following URL:

  http://www.cisco.com/en/US/docs/ios/12_1t/12_1t1/feature/guide/dtasyncq.html

  Workaround: Unconfigure refuse-message in line configuration if a line or a range of lines is part of rotary group without Async call queuing capability.

- CSCdv36885

  A Cisco router may experience a software-forced reload at PC 0x602E7660 and display the following message on the console log:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout
  ```

This condition may occur if a network of routers is configured in a mesh such as a configuration with Response Time Reporter (RTR) jitter probes and with overlapping source and destination ports.

For example if you have three routers A, B, and C with IP addresses 10.1.1.1, 10.2.2.2, and 10.3.3.3 respectively, the configuration for each router is shown as follows:

Router A:

```
rtr responder
rtr 1 type jitter dest-ipaddr 10.2.2.2 dest-port 99
source-ipaddr 10.1.1.1 source-port 99
rtr schedule 1 life forever start-time now
rtr 2 type jitter dest-ipaddr 10.3.3.3 dest-port 99
source-ipaddr 10.1.1.1 source-port 99
rtr schedule 2 life forever start-time now
```

Router B:

```
rtr responder rtr 1 type jitter dest-ipaddr 10.1.1.1 dest-port 99
source-ipaddr 10.2.2.2 source-port 99
rtr schedule 1 life forever start-time now
rtr 2 type jitter dest-ipaddr 10.3.3.3 dest-port 99
source-ipaddr 10.2.2.2 source-port 99
rtr schedule 2 life forever start-time now
```

Router C:

```
rtr responder rtr 1 type jitter dest-ipaddr 10.2.2.2 dest-port 99
source-ipaddr 10.3.3.3 source-port 99
rtr schedule 1 life forever start-time now
rtr 2 type jitter dest-ipaddr 10.1.1.1 dest-port 99
source-ipaddr 10.3.3.3 source-port 99
rtr schedule 2 life forever start-time now
```

Workaround: Configure each source port to be unique and change every destination port so that it does not overlap with any source port (destination ports do not have to be unique).

- CSCdv54045

  A slow memory leak may occur when the DocsDevNmAccessTable is accessed. There is no workaround.

- CSCdv63331

  Out of sequence ATM adaptation layer 1 (AAL1) frames and invalid parity bits may occur if structured circuit emulation service (CES) is configured on a Cisco MC3810 multiaccess concentrator that has a multiflex trunk module (MFT). There is no workaround.

- CSCdv75121

  Symptoms A master Route Switch Processor (RSP) may cause a router to pause indefinitely or reload.

  Conditions This symptom is observed on a Cisco 7500 series router that is configured with a line card when the **write memory** EXEC command is entered and when the line card reloads while the **write memory** EXEC command is being processed.

  Workaround There is no workaround.

- CSCdv85396

  A Cisco 2611 router that is running Cisco IOS Release 12.1(5)T9 or Release 12.2(5a) with generic traffic shaping may reload every 2 minutes because of a segmentation violation exception error. A stack trace similar to the following may be displayed:

```
System was restarted by error - a SegV exception, PC 0x8042B0AC at 05:39:58 UTC C2600
Software (C2600-IO3-M), Version 12.1(5)T9, RELEASE SOFTWARE (fc1) TAC Support:
http://www.cisco.com/tac (current version) Image text-base: 0x80008088, data-base:
0x809BF854

Stack trace from system failure: FP: 0x810DB248, RA: 0x8042AEB8 FP: 0x810DB260, RA:
0x80028884 FP: 0x810DB298, RA: 0x80028F1C FP: 0x810DB2B0, RA: 0x80377C2C FP:
0x810DB300, RA: 0x80467618 FP: 0x810DB340, RA: 0x8045681C FP: 0x810DB358, RA:
0x8045790C FP: 0x810DB398, RA: 0x80455F04
```

This condition occurs in the following scenarios:

- An NM-4 BRI card is in the slot.
- The **access-list 165** command is applied to dialer 5.
- Traffic shaping is applied to Ethernet interface 0/0 when four channels of two BRI interfaces are connected in a multilink bundle and are passing a significant amount of traffic.

Workaround: Remove the **traffic-shape** command on Ethernet interface 0/0.

- CSCdw02017

  Symptoms An EVENT-MIB set action may not work correctly.

  Conditions This symptom is observed when the Simple Network Management Protocol (SNMP) read-write community string is not set correctly. For EVENT-MIB set actions to occur correctly the SNMP read-write community string must be set in mteEventSetContextName.

  Workaround Use mteEventSetContextName for specifying the community name.

- CSCdw09442

  The Route Processor Module (RPM-PR) bootflash is corrupted, and an invalid file header magic number is generated. The **dir** command does not work. The Flash memory can be read after a squeeze bootflash operation is performed, but nothing can be copied onto the Flash memory.

  Workaround: Format and copy files from the disk to recover the Flash memory.

- CSCdw11198

  A Cisco router may reload when a probe is configured to operate at a frequency of 0 seconds and then is scheduled to run.

  Workaround: The probe frequency of 0 seconds is illegal and must not be used.

- CSCdw18318

  A vendor-specific client may cause Link Control Protocol (LCP) to be renegotiated. When authentication, authorization, and accounting (AAA) accounting send stop-record authentication failure is configured, PPP and AAA may cause two sets of accounting records to be generated (one START/STOP record for the final good call and one STOP record for the first setup attempt that was interrupted for the renegotiation). This behavior creates a problem because two sets of accounting records are based on the same call. Users expect only one STOP record for every call in a dial environment. This behavior may impact back-end statistics. There is no workaround.

- CSCdw20082

  An inability to push different accounting records to different server groups prevents a customer from properly segregating vendor-specific callers from other callers. This capability is already supported for EXEC and network accounting and other accounting types but not for resource accounting using method lists. There is no workaround.

- CSCdw30178

  Symptoms A Cisco router may not be accessible through the Ethernet 0 interface.

Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.0(20.3)S1

Workaround Load the software onto the router, copy the running configuration file to the startup configuration, and reload the router.

- CSCdw30258

  When the **write memory** command is used on a Cisco 7500 router that has High System Availability (HSA) with two Route Switch Processors (RSPs) while the **service sync config** command or the **slave sync config** privileged EXEC commands is configured on the same system, the master RSP will cause the CPU to run at 100 percent. The duration of time at which the CPU will run at 100 percent depends on the size of the configuration. This behavior may cause timeouts for pings, Telnet, the Simple Network Management Protocol (SNMP), and other low priority tasks. Higher priority tasks on the router are not affected. There is no workaround.

- CSCdw42868

  Symptoms A router may reload after the **frame-relay payload-compress frf9 stac** interface configuration command is configured on a port adapter interface.

  Conditions This symptom is observed on a Cisco 7500 router that has a 4-port serial port adapter (PA-4T+) and that is running the Route Switch Processor (RSP) software RSP-ISV-M of Cisco IOS Release 12.1(10)E. This symptom does not occur if a Fast Serial Interface Processor (FSIP) is used.

  Workaround Use a FSIP or enter the **frame-relay payload-compression frf9 stac software** interface configuration command on the serial port adapter interface.

- CSCdw44030

  Symptoms The permanent virtual connection (PVC) for an ATM subinterface is created but not activated.

  Conditions This symptom is observed when a router is booting up.

  Workaround To activate the PVC, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM interface.

- CSCdw45491

  Symptoms A route may be parsed incorrectly, which causes an error when the route is applied, and causes a call to be dropped.

  Conditions This symptom is observed when a RADIUS user profile contain an “ip:route” vendor-specific attribute (VSA) that itself contains Virtual Private Network routing and forwarding (VRF) information.

  Workaround There is no workaround.

- CSCdw51935

  Symptoms When serial interfaces that use Frame Relay are configured, the following messages may be displayed:

  ```
  %RSP-3-BADBUFHDR: freeing MEMD pak, address 0 -Traceback= 603A0098 603A7D98 603AD718
  603B35F0 6035CA0C
  %RSP-3-BADBUFHDR: freeing MEMD pak, address 0 -Traceback= 603A0098 603A7D98 603AD718
  603B35F0 6035CA0C
  ```

  If the messages are displayed repeatedly, the router must be reloaded to return to normal working condition.

  Conditions This symptom is observed after Frame Relay-fragmented packets that are selected for selective packet discarding are reassembled.

  Workaround There is no workaround.

- CSCdw52694

  Symptoms Attempts to restart or reschedule an active response time reporter (RTR) probe. Attempts to do so result in the probe being shown with a status of "Unknown" when the **show rtr operation** command is executed.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround Enter the **no rtr** command and reconfigure the RTR probe. Note that the **no rtr** command will disable all of the RTR probes and must be used with utmost caution.

- CSCdw52832

  Symptoms A Cisco router boots the boot image in bootflash instead of booting the full Cisco IOS image from the disk.

  Conditions This symptom is observed when all of the following conditions are met:

  – The configuration register is set to autoboot.

  – There is no configuration in the NVRAM.

  – The **boot system** command is not in the configuration.

  – There is a complete and bootable Cisco IOS image on the disk, and there is a boot image in bootflash.

  Workaround Set the router to boot the image from the disk using the **boot system** global configuration command.

- CSCdw55475

  Symptoms The "octets in" (ifHCInOctets) counters and "octets out" (ifHCOutOctets) counters may fluctuate wildly and display erroneous values when a Simple Network Management (SNMP) query is performed. The following is a sample output of the SNMP query of the ifHCInOctets and ifHCOutOctets counters:

  ```
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.6.9 : Counter64: 746173285208
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.6.9 : Counter64: 1953276477
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.6.9 : Counter64: 746222312654
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.6.9 : Counter64: 8095024725
  ```

  Conditions These symptoms are observed on the E1 and ATM interfaces on a Cisco 7200 series or Cisco 7500 series router. 64-bit counters should not be used because the speed of the E1 and ATM interfaces are lower than 20 Mbps. Erroneous 64-bit values are returned for these low speed interfaces if an SNMP query of the ifHCInOctets and ifHCOutOctets counters is performed while using a running configuration that has the **snmp-server sparse-tables** global configuration command configured.

  Workaround Use 32-bit ifInOctets and ifOutOctets counters for low speed interfaces and 64 bit ifHCInOctets and ifHCOutOctets counters for high speed interfaces.

  Alternate Workaround Enter the **no snmp-server sparse-tables** global configuration command.

- CSCdw61094

  Symptoms A Cisco router may display the following traceback messages and reload after the **clear cdp table** privileged EXEC command is issued:

  ```
  %ALIGN-3-TRACE: -Traceback= 604E42A0 604E39EC 604E37B0 604E32B0 6026BDE4 60277FCC
  602C90F4 602C90E0
  %ALIGN-3-TRACE: -Traceback= 604E42CC 604E39EC 604E37B0 604E32B0 6026BDE4 60277FCC
  602C90F4 602C90E0
  %ALIGN-3-TRACE: -Traceback= 604E42D0 604E39EC 604E37B0 604E32B0 6026BDE4 60277FCC
  602C90F4 602C90E0
  ```

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.1(12).

Workaround There is no workaround.

- CSCdw78024

  Symptoms An access server may reload because of a bus error that is related to an exception that occurs in the authentication, authorization, and accounting (AAA) process when this process is configured to work with method lists.

  Conditions This symptom is observed on an access server that is running Cisco IOS Release 12.2 and that is serving analog ISDN users for Virtual Private Dialup Network (VPDN) Layer 2 Tunneling Protocol (L2TP) connectivity via TACACS+ and RADIUS.

  Workaround There is no workaround.

- CSCdw82465

  Symptoms The **aaa accounting send stop-record authentication failure** global configuration command may send two stop records per call.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw89098

  Symptoms During a default Virtual Private Dialup Network (VPDN) authorization, the following error may be generated:

  ```
  %AAAA-3-NOLIST: AUTHOR/VPDN (1020598405): no method list-name.
  ```

  The default authorization may return a “NULL” method name instead of a “default.” This situation causes the error message.

  Conditions This symptom is observed on a Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC).

  Workaround Define a nondefault method list on the interface over which the call occurs so that a default is not presumed.

- CSCdw90549

  Symptoms The AAA Preauthentication feature may not function properly. The Link Control Protocol (LCP) authorization process may fail and a session is terminated.

  Conditions This symptom is observed in Cisco IOS Release 12.2(6) or Release 12.2(7a).

  Workaround There is no workaround.

- CSCin02000

  Symptoms If you add new interfaces on a line card, the Multicast Distributed Fast Switching (MDFS) functions on other line cards of the same router do not recognize the newly added interfaces until multicast is enabled on the newly added interfaces.

  Conditions This symptom is observed on a Cisco 12000 series.

  Workaround Turn on a multicast function, such as the Protocol Independent Multicast (PIM) mode.

EXEC and Configuration Parser

- CSCdw53946

  Symptoms A router may reload unexpectedly.

Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.1.(12) and that has Network Time Protocol (NTP) configured when a configuration change is made by a user whose username has a percent (%) sign in it.

Workaround There is no workaround.

IBM Connectivity

- CSCds80112

  Symptoms A Cisco router may reload when the data-link switching plus (DLSw+) Ethernet Redundancy feature is used.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.1 only when the **dlsw transparent map** interface configuration command is configured.

  Workaround There is no workaround.

- CSCdw50296

  Symptoms A Cisco 7200 series router that is configured with data-link switching plus (DLSw+) Routing Information Field (RIF) pass-through peers may reload.

  Conditions This symptom is observed when the reachability for a given MAC address has at least two local physical interfaces:

  – The DLSw reachability cache is in the VERIFY state.

  – The combined local and remote RIF length exceeds the maximum number of transmission hops that are allowed in a RIF.

  Workaround Perform the following steps:

  a. Ensure that the combined RIF length does not exceed seven hops. Configure both ends of the RIF pass-through peer on the physical Token Ring interfaces using the following interface configuration commands:

  ```
  source-bridge max-hops 3
  source-bridge max-in-hops 3
  ```

  These commands limit the maximum number of hops from each end of the physical Token Ring interface to three hops. An additional fourth hop is used for the virtual ring. This configuration keeps the combined RIF length to within seven hops.

  b. Ensure that the verify timer is larger than the cache timeout to avoid entering the VERIFY state. Enter the following commands in global configuration mode:

  ```
  dlsw timer sna-verify-interval 1200
  dlsw timer netbios-verify-interval 1200
  ```

  These commands set the verify interval to 20 minutes (the default cache timeout is 16 minutes, or 960 seconds). This configuration prevents the router from entering the VERIFY state. The cache entry is deleted before the router can perform a VERIFY operation.

Interfaces and Bridging

- CSCdv04951

  A Cisco 7200 series router may reload when it is passing a heavy traffic of large packets through a PA-A1 port adapter. The reload does not occur under normal traffic conditions.

Possible workaround: Reduce the maximum transmission unit (MTU) size of the ATM interface so that the interface never has to pass a packet of more than 4500 bytes.

- CSCdv28626

  Symptoms ATM virtual circuit (VC) counters are not correctly incremented on a 1-port ATM OC-3 multimode port adapter (PA-A1-OC3MM)

  Conditions This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.1(7a)E2.

  Workaround There is no workaround.

- CSCdv76946

  Pings can be sent across Fast Ethernet interfaces that have 802.1q (dot1q) encapsulation configured. However, if the encapsulation on the subinterfaces are changed to Inter-Switch Link (ISL) on both of the routers, the routers may reload. There is no workaround.

- CSCdv84788

  Symptoms A Versatile Interface Processor (VIP) may reload or record spurious access or record spurious access after class maps are configured for Frame Relay.

  Conditions This symptom is observed on a Cisco 7500 series router.

  Workaround There is no workaround.

- CSCdw28119

  Symptoms On a port adapter, some of the permanent virtual connections (PVCs) may not work properly. Consequently, some of the switched virtual circuits (SVCs) may not come up properly.

  Conditions This symptom is observed on a PA-A1 port-adaptor on a Cisco 7500 series router that is running Cisco IOS Release 12.2(6.8)T.

  Workaround Enter the **shutdown** interface configuration command to shut down the ATM interface. Wait for approximately 40 seconds, and then enter the **no shutdown** interface configuration command to enable the ATM interface.

- CSCdw39876

  Symptoms A Cisco router that is connected to a Cisco Catalyst 5500 switch may reload with a bus error or enter a constant boot loop. The output from the reload indicates that 802.1q (dot1q) is the cause of this behavior even though the router is not configured for dot1q trunking. The looping stops after the Ethernet cable is physically disconnected from the switch.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(6.7).

  Workaround Configure a native VLAN on the trunk and configure all the protocol attributes on the native VLAN instead of the main interface. The two configurations are equivalent. The advantage of configuring the VLAN as native is that all packets are received and sent as untagged.

- CSCdw44425

  Symptoms A wedged input queue may occur on an ATM interface. Port-based TCP debugging is partially malfunctioning. If a packet is received from a port that is different from the port on which port debugging is enabled, the input queue may become wedged and a packet memory leak may occur.

  The following output may be displayed when the **show interface** EXEC command is issued:

```
ATM4/0 is up, line protocol is up
Hardware is ENHANCED ATM PA
Description: ** HX451039 2Mbit Bankdata erritsxbygade 102 **
MTU 4470 bytes, sub MTU 4470, BW 2000 Kbit, DLY 200 usec, reliability 255/255, txload
1/255, rxload 1/255
```

```
Encapsulation ATM, loopback not set
Encapsulation(s): AAL5
4095 maximum active VCs, 5 current VCCs
VC idle disconnect time: 300 seconds 0 carrier transitions
Last input 00:00:50, output 00:00:05, output hang never
Last clearing of "show interface" counters 00:07:34
Input queue: 76/75/83/0 (size/max/drops/flushes);
Total output drops: 0 <---- Interface wedged
Queueing strategy: Per VC Queueing
30 second input rate 0 bits/sec, 0 packets/sec
30 second output rate 0 bits/sec, 0 packets/sec
    3709 packets input, 316026 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    512 packets output, 35105 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

Conditions This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(6).

Workaround There is no workaround.

- CSCdw47993

  Symptoms A router may reload because of an SegV exception.

  Conditions This symptom is observed when FRF.9 hardware compression is used on a platform that supports hardware compression.

  Workaround Disable hardware compression.

- CSCdw48170

  Symptoms It may not be possible to configure the **clock rate** interface configuration command.

  Conditions This symptom is observed on a Cisco MC3810 that is running Cisco IOS Release 12.1(13) or Release 12.2(6.8).

  Workaround There is no workaround.

- CSCdw49266

  Symptoms A spurious memory access may occur on a Cisco 2600 series, Cisco 7200 series, Cisco 7500 series, or Cisco 12000 series Internet router.

  Conditions This symptom is observed when one of the routers mentioned is running a Cisco IOS release other than Cisco IOS Release 12.1 E that contains the fix for caveat CSCdp70087.

  Workaround There is no workaround.

- CSCdw51050

  Symptoms A spurious memory access may occur on a Cisco router and the router may reload because of a bus error while a tagged packet is process-switched.

  Conditions This symptom is observed on a Cisco router that is using Inter-Switch Link (ISL) encapsulation.

  Workaround Use 802.1q encapsulation. This workaround may require changes for 802.1q encapsulation on the sides of the Ethernet switch and the router because both sides of the LAN should use the same type of encapsulation.

- CSCdw57367

  Symptoms When a router boots up with distributed Cisco Express Forwarding (dCEF) disabled and Cisco Express Forwarding (CEF) enabled, 802.1q packets are fast-switched instead of CEF-switched.

  Conditions This symptom is observed on a Cisco 7500 series router that is running a Cisco IOS image into which either the fix for caveat CSCdu39979 or caveat CSCdv78842 has been integrated.

  Workaround Use dCEF instead of CEF. If you cannot configure dCEF and CEF is the only alternative, perform the following steps:

  a. Enable the **ip cef distributed** global configuration command.

  b. Wait for one minute.

  c. Enable the **ip cef** global configuration command.

- CSCdw60490

  Symptoms A router may use Cisco Express Forwarding (CEF) to switch IP packets that enter an Inter-Switch Link (ISL) subinterface, regardless of the (interior) destination MAC address.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw67214

  Symptoms IP packets that are larger than 1484 bytes are not passed.

  Conditions This symptom is observed on a Cisco 7507 router that is configured with a Versatile Interface Processor 2-40 (VIP2-40) with a dual-port Fast Ethernet port adapter (PA-2FE-TX) and that is configured as an Inter-Switch Link (ISL).

  Workaround There is no workaround.

- CSCdw79641

  Symptoms A channelized T3 Interface Processor (CT3IP-50) may reload with an error message that is very similar to the following:

```
$0 : 00000000, AT : 30037FE0, v0 : 00000000, v1 : 3802F3BE
a0 : 60A6FEA0, a1 : 60A07EA0, a2 : 00000007, a3 : 00000020
t0 : 00008000, t1 : 4E90424C, t2 : 00000001, t3 : 601824C8
t4 : 600C8040, t5 : 000000F8, t6 : 00000000, t7 : 611F7BAC
s0 : 60A07EA0, s1 : 0000000A, s2 : 00000030, s3 : 60A71880
s4 : 00006000, s5 : 60A6FEA0, s6 : 00000033, s7 : 60A49660
t8 : 8E07F138, t9 : 00000000, k0 : 00000000, k1 : 00000004
gp : 606DBFC0, sp : 6086C380, s8 : 00000003, ra : 6017DFB0
EPC : 00000000, ErrorEPC : 800086B8, SREG : 3400E103
Cause 00000008 (Code 0x2): TLB (load or instruction fetch) exception

-Traceback= 0x6017DFB0 0x601805FC 0x601825A4
```

  Conditions This symptom is observed in a Cisco router that is running Cisco IOS Release 12.0(21)S1.

  Workaround There is no workaround.

- CSCdw87343

  Symptoms The following traceback messages may be displayed when Multiprotocol Label Switching (MPLS) Weighted Random Early Detection (WRED) is tested:

```
%IPC-5-SLAVELOG: VIP-SLOT3:

%SYS-2-INLIST: Buffer in list, ptr= 60B3C540 -Process= "<interrupt level>", ipl= 2,
pid= 15
```

```
-Traceback= 600BA170 60165964 60166724
%SYS-2-INLIST: Buffer in list, ptr= 60B39EC0
```

Conditions This symptom occurs when MPLS WRED is tested with WRED configured to use default queue thresholds. Pings that are sent from a Pagent router to a destination fail.

Workaround There is no workaround.

- CSCdw89164

  Symptoms A memory allocation failure (MALLOCFAIL) message is displayed when a cable is unplugged from a serial interface.

  Conditions This symptom is observed on a Cisco 7206VXR router that is running Cisco IOS Release 12.2(7a) and that has a Network Processing Engine (NPE-400). This situation occurs when a cable is unplugged from a serial interface and if **l3 bypass** global configuration command is enabled.

  Workaround There is no workaround.

- CSCdw93032

  Symptoms The s1s0 flag that is configured on Packet-over-SONET(POS) interfaces automatically may reset to 0 after a reload.

  Conditions This symptom is observed on a Cisco 7200 or a Cisco 7500 series router that is running Cisco IOS Release 12.1(9)E.

  Workaround There is no workaround.

- CSCdx27009

  Symptoms An IP ping does not go through on the bridging and the bridging-to-routing path.

  Conditions This symptom is observed in an integrated routing and bridging (IRB) environment. Pings can be sent through the routing and the routing-to-bridging path, but pings cannot be sent through on the bridging and the bridging-to-routing path.

  Workaround There is no workaround.

IP Routing Protocols

- CSCdt62457

  Redistribution may not work as expected when it is configured under the Multicast family for the Border Gateway Protocol (BGP). Some autosummarization may take place instead. There is no workaround.

- CSCdv30330

  A Cisco router that is configured for Multicast Source Discovery Protocol (MSDP) may experience frequent MSDP session resets with the MSDP peers of the router. This situation is often caused by excessive source, group (S, G) information that should be contained in a domain being passed to the outside, resulting in additional entries in the Source-Active (SA) cache.

  Workarounds: Determine if the routers have the SA filters configured properly by reviewing the MSDP SA filter recommendations posted at the following URL:

  ftp://ftpeng.cisco.com/ipmulticast/config-notes/msdp-sa-filter.txt

  Determine if the router is running a Cisco IOS image that has the fix for CSCdr93446 (MSDP: Reducing SA storms and session resets [MSDP rearchitect]).

Review the output of the **show ip msdp sa-cache** EXEC command to see if some of the SAs can be filtered based on the source address, the Rendezvous point (RP) address, or the autonomous system (AS) number.

- CSCdv39749

  Symptoms Unconfiguring the Intermediate System-to-Intermediate System (IS-IS) protocol on a Cisco 12000 series 4-port OC-3 ATM line card may cause the router to reload.

  Conditions This symptom is observed on a Cisco 12000 series Internet router that is running Cisco IOS Release 12.0(17)S.

  Workaround There is no workaround.

- CSCdv65061

  A weight value is changed when the **clear ip bgp** EXEC command is issued. Soft reconfiguration inbound does not work correctly.

  Workaround: Set weight as part of the inbound route map.

- CSCdv71515

  Symptoms The bidirectional flag is not reset on a multicast route (mroute) entry when the group status changes from the bidirectional state to the dense state.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdv81127

  A Traffic Engineering (TE) tunnel may not come up after a router or an interface card on the headend of the TE tunnel is reloaded.

  Workaround: Enter the **shutdown** interface configuration command followed by the no **shutdown** interface configuration command on the interface that is used as an outgoing interface for the TE tunnel at the headend.

- CSCdv89039

  Symptoms A Cisco router may reload because of a bus error at the ipnat_unlock_parent_entry process.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(5).

  Workaround There is no workaround.

- CSCdv89098

  Symptoms A Border Gateway Protocol (BGP) session may time out, and the router may display the following message:

  ```
  %BGP-3-NOTIFICATION: received from neighbor x.x.x.x x/x (hold time expired) 0 bytes
  ```

  Conditions This symptom is observed on a Cisco router that is running Multiprotocol Label Switching (MPLS) on an outbound interface that is connected to the MPLS network core and occurs when a BGP session with a maximum segment size (MSS) that is computed from the maximum transmission unit (MTU) of the next-hop interface of the router has been established and the **ip tcp path-mtu-discovery** global configuration command has been entered.

  Workaround Adjust the IP MTU on one of the BGP routers using the **ip mtu** *bytes* interface configuration command. For example, to enforce a BGP session with a TCP MSS of 4426 bytes, issue the following command:

  ```
  Router(config-if)# ip mtu 4426
  ```

The MTU and the shim header add up in the following way: an MSS of 4426 bytes plus a 40-byte TCP/IP header plus a 4-byte shim header equals 4470 (Packet- over-SONET [POS] link).

- CSCdw02051

  Symptoms Reverse Domain System (DNS) lookup may fail.

  Conditions This symptom is observed if a DNS server is located on the inside of a Network Address Translation (NAT) device while the host is located outside of the NAT device. This symptom occurs if the router is configured with the **ip nat outside source** global configuration command.

  Workaround Relocate the DNS server to the outside of the NAT device.

- CSCdw15323

  The output of the **show ip rsvp reservation** EXEC command displays interface names that are truncated to five digits. This behavior may also occur with the following show commands:

  ```
  show ip rsvp request
  show ip rsvp sender
  show ip rsvp host receivers
  show ip rsvp host senders
  show ip rsvp temp-psb
  show ip rsvp temp-rsb
  ```

  This condition prevents port numbers, such as those on Versatile Interface Processor (VIP) cards, from being displayed fully. This condition occurs when a router is configured with the Resource Reservation Protocol (RSVP) using the **ip rsvp bandwidth** interface configuration command while there is at least one ongoing RSVP session. There is no workaround.

- CSCdw17989

  Symptoms Inconsistent and unpredictable behavior may occur when Protocol Independent Multicast dense mode (PIM-DM) is used on certain point-to-point interfaces.

  Conditions This symptom is observed after the fix for caveat CSCdt87405 has been implemented and is more likely to occur with tunnel interfaces.

  Workaround There is no workaround.

- CSCdw19340

  A Cisco router may reload after the **aggregate-address** command is configured within a Multicast Border Gateway Protocol (MBGP) address family. There is no workaround.

- CSCdw20251

  A Route Switch Processor (RSP) that is running Cisco IOS Release 12.0(20.2)ST may reload when the **show ip mroute** command is executed. There is no workaround.

- CSCdw22714

  A Cisco router may reload if the last network statement for an area is removed from the configuration of an Open Shortest Path First (OSPF) router. There is no workaround.

- CSCdw27874

  Symptoms A memory leak may occur with queues.

  Conditions This symptom is observed when the Enhanced Interior Gateway Routing Protocol (EIGRP) is configured or unconfigured.

  Workaround Remove all the network commands using the **no network** *network-number* router configuration command and then enter the **router eigrp** *autonomous-system-number* global configuration command.

- CSCdw35985

  Symptoms Enhanced Interior Gateway Routing Protocol (EIGRP) may cause an unexpected system reload at the igrp2_bandwidth_changed process.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw36746

  A Cisco router may reload because of a bus error at an invalid address if Open Shortest Path First (OSPF) is enabled and if the same interarea prefix is advertised from multiple areas and is more than the *path* argument of the **maximum-path** *path* command that exist in the interarea prefix. There is no workaround.

- CSCdw60555

  Symptoms A Cisco router that has Network Address Translation (NAT) configured may reload with a bus error.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(3).

  Workaround There is no workaround.

- CSCdw61134

  Symptoms Network Address Translation (NAT) fails to translate H.245 packets. This situation causes one-way voice traffic.

  Conditions This symptom is observed when H.225 and H.245 traffic originates from different address sources.

  Workaround There is no workaround.

- CSCdw75860

  Symptoms Cisco IOS Release 12.2 and earlier releases may not be able to interoperate.

  Conditions This symptom is observed when you configure an invalid encrypted password for Open Shortest Path First (OSPF) message digest algorithm 5 (MD5) authentication. An error message is generated to warn the user of the invalidly entered password.

  For example, when you enter the **ip ospf message-digest-key** *key-id* **md5** *key* interface configuration command, the message "OSPF: Invalid encrypted password: *key*" is generated, in which *key* is the invalidly entered password.

  Workaround There is no workaround.

- CSCdw77775

  Symptoms A router may reload.

  Conditions This symptom is observed on a Cisco router when a large Network Address Translation (NAT) address pool is unconfigured.

  Workaround There is no workaround.

- CSCdw82101

  Symptoms With Enhanced Interior Gateway Routing Protocol (EIGRP) enabled, if the **summary-address** router configuration command is configured on a virtual template, EIGRP sends individual specific routes within the summary-address range instead of the summarized routes as configured. Also, EIGRP may not send any specific routes, nor summarized routes.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround Configure an outbound distribution list to deny all specific routes.

- CSCdw83531

  Symptoms Border Gateway Protocol (BGP) updates may be corrupted. The following message may be displayed when this symptom occurs:

  ```
  BGP-6-NEXTHOP: Invalid next hop (0.0.0.0) received from x.x.x.x: martian next hop
  BGP(0): x.x.x.x rcv UPDATE w/ attr: nexthop 0.0.0.0, origin ?, metric 0, originator
  0.0.0.0, path YYYY, community , extended community
  20.1.1.0/24 -- DENIED due to: martian NEXTHOP;
  ```

  Conditions These symptoms are observed on a customer edge (CE) router when BGP updates are sent from a provider edge (PE) router to the CE router if peer groups are specified using the **address-family ipv4 vrf** *vrf-name* router configuration command. BGP routes may be lost on the CE router even though the BGP neighbors remain up.

  Workaround Remove the peer group configuration from the **address-family ipv4 vrf** *vrf-name* router configuration command.

- CSCdx04476

  Symptoms When Network Address Translation (NAT) is configured in interface overload mode, an IP packet should not be processed by the router as if it were destined for the router. However, after the NAT deciphering of the Internet Control Message Protocol (ICMP) notification, an unnecessary RST (reset flag in the TCP header) message is sent after the ICMP “type 3 code 4” message, resulting in the closure of the TCP dialog without notifying the end station behind the NAT router.

  Conditions This symptom is observed in a Cisco IOS release that contains the fix for caveat CSCdu70301.

  Workaround Use a Cisco IOS release that does not contains the fix for caveat CSCdu70301, that is, a Cisco IOS release earlier than Cisco IOS Release 12.2(4.2).

- CSCdx06621

  Symptoms A router may reload with a bus error while the shortest path first (SPF) algorithm is computed.

  Conditions This symptom is observed if multiple routers are advertising the same prefix in Type-5 or Type-7 link-state advertisements (LSAs).

  Workaround There is no workaround.

- CSCdx33019

  Symptoms A router may reload.

  Conditions This symptom is observed when two paths to the same destination network are withdrawn simultaneously.

  Workaround There is no workaround.

- CSCin02516

  Symptoms When you enter the **no ip address** interface configuration command on an interface, the associated adjacency entries are not removed. When a previous interface IP address is reassigned on a subinterface of the same interface, the nonremoved adjacency entry that is still pointing to the previous interface is associated with this IP address.

  Conditions This symptom is observed on static Address Resolution Protocol (ARP) entries that have their IP addresses on the same subnet as the interface.

  Workaround Remove the static ARP configuration.

- CSCin03316

  Symptoms A Resource Reservation Protocol (RSVP) session that requests traffic control quality of service (QoS) leaks approximately 1.3 KB of memory when the session ends. The memory leak does not depend on the duration of the session, and the memory leak occurs on all Cisco routers along the session path. The rate of the memory loss is proportional to the rate at which RSVP sessions are created and terminated.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

ISO CLNS

- CSCdu52672

  With Multiprotocol Label Switching (MPLS) traffic engineering, when a link on a tunnel headend is protected with Fast Reroute (FRR), 40 to 120 milliseconds of traffic may be lost for traffic that have destinations that go through the tunnel that are learned using auto route. The loss of traffic occurs after the FRR process has taken place. This condition occurs because the prefix is removed from the routing table after the first Shortest Path First (SPF) trigger is received. The prefix is readded after the SPF calculation is completed.

  Workaround: Implement one of the following workarounds:

  d. For Cisco IOS images that have the Intermediate System-to-Intermediate System (IS-IS) backoff algorithm, assign short intervals when using the **prc-interval** *seconds* router configuration command to reduce the delay.

  e. Use forwarding adjacencies. This workaround will prevent packet traffic loss because the shortest path tree will not change. (if you run i-shortest path first [SPF], the SPF computation time will be less than 1 ms regardless of the topology size). Forwarding agents (FAs) are used to advertise tunnels into the Interior Gateway Protocol (IGP) using a fixed metric. Therefore all routers in the area will see the traffic engineering (TE) tunnel as a normal adjacency. If the tunnel changes path, from an SPF perspective there are no changes and nothing is done on the routing information base (RIB) with Cisco Express Forwarding line cards.

- CSCdw31942

  Symptoms The Intermediate System-to-Intermediate System (IS-IS) interface configuration may be lost.

  Conditions This symptom is observed when a Cisco 12000 series line card is reloaded with microcode.

  Workaround Manually reconfigure the interface configuration.

- CSCdw51855

  Symptoms Two routers may fail to reestablish a Connectionless Network Service (CLNS) relationship after a Packet-over-SONET (POS) outage has occurred between them.

  Conditions This symptom is observed on routers that are running Cisco IOS Release 12.0(18)S.

  Workaround Enter the **clear isis *** command on the routers.

- CSCdw82849

  Symptoms When you unconfigure the Intermediate System-to-Intermediate System (IS-IS) routing process by entering the **no router isis** global configuration command, the following error message may be generated:

  ```
  WST: %CLNS-1-LINKERR: ISIS: LSP back/front inconsistent in 0x49867AFC, lsp_next
  0x44E1B79C, lsp_prev 0x4375387C, index 40, ver 27, front 0x15A3C78B
  ```

  In rare occasions, the router may reload.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(7.4), Release 12.2(7.4)T, or a later 12.2 or T-train release.

  Workaround There is no workaround.

Miscellaneous

- CSCdk67967

  Symptoms A router may reload at mdfs_reload_process.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdm25278

  In Cisco IOS Releases 12.0 and 12.1, the multichannel T1/E1 port adapters show the Layer 1 status in the ACTIVE state in the **show isdn status** [*output*] EXEC command even after the D channel is shut down.

  Workaround: Shut down the T1 or E1 controller.

- CSCds76314

  Symptoms A permanent virtual connection (PVC) may go from active status to inactive status and display "%ATMCES-1-ERRCREATEVC" error messages.

  Conditions This symptom is observed when the following sequence of commands is entered on a subinterface:

  a. (config-subif)# **shut**
     (config-subif)# **shutdown**
     (config-subif)# **no shut**
     (config-subif)# **no shutdown**
  b. The PVC configuration mode is entered and then exited by entering the **end** EXEC command.

  Workaround Reconfigure the PVC or reload the router.

- CSCdt04135

  When a port from a Ethernet Switch 10BASE-T and 100BASE-TX port adapter (PA-12E/2FE) is used for bridging, all ports in the same bridging group enter the forwarding mode. The spanning tree is not working properly. When the module is replaced with another Ethernet module, one port in the spanning tree loop enters the blocking mode. This behavior is observed on Cisco IOS Release 12.1(2)E. There is no workaround.

- CSCdt25417

  Symptoms A router may pause indefinitely if it cannot send through an 8-port asynchronous and synchronous network module (NM-8A/S).

  Conditions This symptom is observed on a Cisco 3640 router.

  Workaround There is no workaround.

- CSCdt55868

  In rare circumstances, an attempt to load an instruction from 0x0 may cause the router to reload when a router is running images other than service provider and enterprise images.

  Workaround: Run “j” or “p” images.

- CSCdt63578

  Symptoms I/O memory leaks and bus error reloads may occur on a Cisco 7200 series router.

  Conditions This symptom is observed on a Cisco 7200 series router that is configured with a Network Services Engine 1 (NSE-1) and that has Parallel Express Forwarding (PXF) enabled.

  Workaround Apply the **no fair queue** interface configuration command to the affected serial interface.

- CSCdt68781

  Symptoms The **show call resources voice** EXEC command is not available on a Cisco 7200 series router.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdu35097

  Symptoms The byte counters on a serial interface on a Cisco 7500 series router may not operate properly. There is a difference between the number of bytes on one side of a serial link and the number of bytes on the other side of the link. The counter may also decrease.

  Conditions These symptoms are observed on a Cisco 7500 series router that is running Cisco IOS Release 12.1(8).

  Workaround There is no workaround.

- CSCdu48008

  Symptoms The Cable Media Access Control (CMAC) process memory allocation grows because of a T4 timeout or some other cause every time a cable interface is reset. The total amount of free memory decreases by 2000 bytes with each reset.

  Conditions This symptom is observed when docsDecNmAccess entries are included in the Data-over-Cable Service Interface Specification (DOCSIS) configuration file.

  Workaround There is no workaround.

- CSCdu53023

  The IfTable is not updated with the ATM information layer when a new ATM card is inserted.

  Workaround: Reload the router.

- CSCdu55250

  Symptoms Platforms that are configured with fast CPUs may fail to boot if the Cisco IOS image is loaded from a 48-MB or a 128-MB Advanced Technology Attachment (ATA) SanDisk Personal Computer Memory Card International Association (PCMCIA) card, and the following error message is displayed (in which "x" is a digit):

  ```
  ATA_Status time out waiting for x
  ```

  This situation causes the platform to return to the ROM monitor (ROMmon) prompt.

  Conditions This symptom is observed randomly and intermittently and does not occur on cards of other capacities than 48 MB or 128 MB, nor on linear Flash PCMCIA cards.

  The situation is caused by random and intermittent internal noise on the ATA SanDisk PCMCIA card, which causes it to occasionally respond slowly to a read request when loading a Cisco IOS image, and occurs on platforms with fast CPUs because the amount of time that the system waits for the ATA SanDisk PCMCIA card to return the data is less than on platforms with relatively slower CPUs.

  Workaround Do not boot the Cisco IOS image from another device, or use a linear Flash PCMCIA card.

- CSCdu60558

  A Cisco router that is running Cisco IOS Release 12.0(16.6)ST may reload if the **clear ip bgp *** privileged EXEC command is issued repeatedly. There is no workaround.

- CSCdu66206

  Symptoms Multicast Output interfaces (OIFs) are missing from certain groups, causing multicast traffic to be affected.

  Conditions This symptom is observed during startup because of the varying speeds in which the cards are turned on.

  Workaround Reload the microcode on the card that contains the missing OIFs. Note that reloading the microcode may lead to issues that are related to caveat CSCuk22826.

- CSCdu71743

  Symptoms A Cisco router may reload with a stack trace that points to the authorization proxy.

  Conditions This symptom is observed on a Cisco 2600 series router that is running Cisco IOS Release 12.1(5)T9.

  Workaround If possible, disable the authorization proxy.

- CSCdu72839

  Symptoms If you configure and then unconfigure an ATM bundle on an interface, the interface may stop forwarding traffic.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdu74983

  Users that have links that utilize external encryption gear have to use the **pulse-time** *seconds* interface configuration command in order for the router interface to transition the data terminal ready (DTR) to resynchronize the encryption equipment. When a user is using Enhanced Interior Gateway Routing Protocol (EIGRP) and performs a router reload, one or more of the serial interfaces with the **pulse-time 1** command or **pulse-time 2** command configured does not show up in the EIGRP topology table. Individual serial interfaces with different clock rates that have the **pulse-time 2** command configured may also fail to show up in the EIGRP topology table.

Workaround: Enter the **shut** command followed by the **no shut** command on the serial interface that has the problem to reset and force the interface into the EIGRP topology table.

Alternate workaround: Configure the **pulse-time 3** interface configuration command on all serial interfaces.

- CSCdu83462

  A Cisco 7206VXR router that is running Cisco IOS Release 12.2(1) and that has Cisco Express Forwarding (CEF) and Parallel Express Forwarding (PXF) enabled on port channels may experience dropped packets when the router is passing IP traffic. This condition was observed on a Cisco 7206VXR router that was running two port channels across two Fast Ethernet Inter-Switch Link (FE/ISL) port adapters.

  Workaround: Disable CEF using the **no ip route cache** interface configuration command on the FEISL port adapters.

- CSCdu87454

  Symptoms The following messages and tracebacks are generated when the **no dspint dspfarm** global configuration command is entered:

  ```
  %VTSP-3-DSP_TIMEOUT: DSP timeout on event 86: DSP ID=0x1: DSP error stats
  %SYS-3-TIMERNEG: Cannot start timer (0x62A52A70) with negative offset (-84215096).
  -Process= "VTSP", ipl= 0, pid= 90
  -Traceback= 603E6200 603E3E30 60F5BA90 60F66CD4 60F7ED78 60F7F530 60F7025C 60F70850
  603CF324 603CF310
  %VTSP-3-DSP_TIMEOUT: DSP timeout on event 86: DSP ID=0x1: DSP error stats
  ```

  Conditions This symptom is observed when a connection trunk is configured and all the trunk are up.

  Workaround There is no workaround.

- CSCdu88006

  Symptoms A bus error may cause a router to be returned to the ROM mode.

  Conditions This symptom is observed on a Cisco 7204VXR router that is running Cisco IOS Release 12.1(7). The Cisco 7204VXR returns to the ROM mode if the **snasw dump all** privileged EXEC command (or the **snasw dump summary-ipstrace** privileged EXEC command) and the **snasw stop** privileged EXEC command are entered simultaneously on the router.

  Workaround There is no workaround.

- CSCdv01350

  Symptoms Internet Group Management Protocol (IGMP) mtrace response packets (with a protocol value of 2 and an IGMP type of 0x1E) may stay in an interface input hold queue indefinitely. These packets may eventually fill up the interface input hold queue and cause packet drops.

  Conditions This symptom is observed on a Cisco switch or router that is running Cisco IOS software.

  Workaround Reload the router to clear the packets from the input hold queue, and increase the input hold queue depth using the **hold-queue** *length* interface configuration command.

- CSCdv05014

  Symptoms The output of an 8-port serial X.21 port adapter (PA-8T-X21) may be frozen.

  Conditions This symptom is observed on a PA-8T-X21 port adapter that is installed in a Cisco 7500 series Versatile Interface Processor 2-50 (VIP2-50.)

  Workaround There is no workaround.

- CSCdv24563

  A Cisco AS5800 universal access server may experience a memory leak in the pool manager process. There is no workaround.

- CSCdv30027

  If a circuit emulation service (CES) permanent virtual connection (PVC) is created in advance, the **connect** command does not connect the PVC to a T1 time-division multiplexing (TDM) group. There is no workaround.

- CSCdv33361

  Symptoms A spurious access may occur at the "t_acl_list_modified" function in a Versatile Interface Processor (VIP) slot.

  Conditions This symptom is observed after you have configured a distributed access control list (ACL) on a Cisco 7500 series router.

  Workaround Configure a centralized ACL.

- CSCdv33444

  Symptoms Calls cannot be made on a Cisco 7206VXR router that is configured with an enhanced digital voice port adapter (PA-VXC-2TE1) after the port adapter is removed and reinserted. A "call disconnect cause 0x22 no circuit" message is displayed when this condition occurs.

  Conditions This symptom is observed when you perform an online insertion and removal (OIR) of the PA-VXC-2TE1.

  Workaround Reload the router after the OIR of the PA-VXC-2TE1.

- CSCdv38148

  Circuit Emulation Services (CES) does not function properly on a Cisco 3600 series router that is running Cisco IOS Release 12.1(5)T or later releases. There is no workaround.

- CSCdv38529

  When a voice connection trunk is configured between a Cisco 7500 and a Cisco 3600 router and both of the routers are configured for the connection trunk in the master mode (default), traceback messages may appear on the console of the Cisco 7500 router if the Cisco 3600 router starts up before the Cisco 7500 router. When this condition occurs, the trunk channels are not connected. This condition does not occur if the Cisco 7500 is the first router to start up. There is no workaround.

- CSCdv40407

  Symptoms A Cisco router may reload when a ds0 group is unconfigured while there is heavy call traffic (such as when there are numerous calls being set up and torn down).

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround Before unconfiguring the ds0 group, enter the **shutdown** interface configuration command on the controller or the voice port that is associated with the ds0 group.

- CSCdv43014

  With SNA Switching Services (SNASw), some downstream physical units (PUs) may remain in the reset state and cannot be activated. The **show snasw pu** EXEC command or **show snasw dlus** EXEC command may show that the Dependent Logical Unit Requestor/Dependent Logical Unit Server (DLUR/DLUS) pipe is in the Pend Inact state. Digital loop carrier (DLC) traces may also show no activity on this pipe.

  Workaround: Restart SNASw.

- CSCdv44349

  When Connectionless Network Service (CLNS) traffic is sent through an ATM permanent virtual circuit (PVC), a spurious access occurs in hqf_vip_decode_encaps. There is no workaround.

- CSCdv44860

  Symptoms Configuring "set" under a main interface service policy has no effect on subinterface traffic. Packets switching out of a subinterface are classified correctly by the policy, but the "set" counter does not increment.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround Apply the policy map to the subinterface.

- CSCdv46696

  Symptoms Sometime after performing an online insertion and removal (OIR) of a Cisco 7000 series Versatile Interface Processor (VIP), all distributed Multilink PPP (dMLP) traffic may stop flowing.

  Conditions This symptom may occur several minutes after an OIR or one day after an OIR.

  Workaround Reload the router.

- CSCdv47546

  Symptoms A gradual memory leak may occur on a Cisco AS5300 that is used as a Voice over IP (VoIP) gateway.

  Conditions This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(1a).

  Workaround There is no workaround.

- CSCdv48025

  Symptoms A fast cache entry may get built when inbound NetFlow is configured on top of Cisco Express Forwarding (CEF) on an Ethernet interface.

  Conditions This symptom is observed on a Cisco Route Switch Processor (RSP) that is running Cisco IOS Release 12.2 or Release 12.2 T with an Ethernet to Fast Ethernet channel combination topology.

  Workaround There is no workaround.

- CSCdv48137

  A Cisco router may lose a configuration (such as a BRI configuration) when the router is reloaded.

  Workaround: Reapply the lost configuration.

- CSCdv50458

  A Cisco Route Switch Module (RSM) that is running Cisco IOS Release 12.0(16) may experience memory allocation (MALLOC) failures that point to Cisco Express Forwarding (CEF) as the process even after CEF has been disabled. There is no workaround.

- CSCdv53233

  Symptoms The console of a Cisco AS5800 router shelf may display several "No active radius servers found" messages followed by "Radius server is responding again" (previously dead) messages. This condition does not impact service.

  Conditions This symptom is observed when the server is working normally and authenticating users.

  Workaround Remove the **radius-server deadtime** *minutes* global configuration command from the router.

- CSCdv53465

  Symptoms A variable bit rate non-real time (VBR-NRT) connection drops traffic when the traffic falls below the sustainable cell rate (SCR).

  Conditions This symptom is observed on a Variable bit rate-non-real time (VBR-NRT) connection with a peak cell rate (PCR) of 50 and an SCR of 25 between two Route Processor Modules (RPMs) when traffic flows at about 20 kbps.

  Workaround There is no workaround.

- CSCdv54509

  A "SYS-3-INVMEMINT: Invalid memory action (malloc)" at interrupt level message may be displayed when an X.75 call is made on an E1 or PRI interface. This behavior has no user impact. There is no workaround.

- CSCdv55967

  Symptoms The error message "%TRUNK-3-HBEAT: No longer receiving heartbeats from framer CPU" may be displayed.

  Conditions This symptom is observed on a Cisco AS5800.

  Workaround Use the firmware that is compiled using the version 96q1 compiler.

- CSCdv57950

  Symptoms The Diffie-Hellman (DH) key pairs are not released, cannot be rekeyed, and cause tunnel failures.

  Conditions These symptoms are observed on a Cisco 7200 series router after a tunnel negotiation.

  Workaround Reload the router.

- CSCdv60937

  Forwarding Information Base (FIB) tables on distributed Cisco Express Forwarding (dCEF) line cards are not cleared when the **clear ip route** * EXEC command is entered. A specific route can still be cleared using the **clear ip route** *prefix* EXEC command.

  Workaround: Shut down all interfaces and remove all the routes on the line cards.

- CSCdv61415

  Symptoms If you enter the **show cot request** *hardware-unit ds0* EXEC command, a Cisco AS5400 may reload if a voice call is active on the DS0 connection. The Continuity Test (COT) type is a 100-percent transponder or loop.

  Conditions This symptom is observed on a Cisco AS5400 that is functioning as a gateway in a Signaling System 7 (SS7) Interconnect for Voice Gateways environment and that is running Cisco IOS Release 12.2(2)XA or Release 12.2(2)XB.

  Workaround Do not use the **show cot request** *hardware-unit ds0* EXEC command when a particular channel is specified.

- CSCdv62424

  A port that has been marked as BAD by system processing engine (SPE) modem recovery after a call failure cannot be recovered using the **clear spe** EXEC command. Calls cannot be placed to the port.

  Workaround: Issue the **clear port** EXEC command.

- CSCdv62572

  A Cisco 3640 router that is running Cisco IOS Release 12.2(5) with a compression module may experience a buffer leak in the normal pool and display the following statistics in the public pool:

```
Public particle pools: Normal buffers, 1548 bytes (total 2535, permanent 512): 0 in
free list (128 min, 1024 max allowed) 770349 hits, 68394 misses, 2095 trims, 4118
created 5705 failures (0 no memory) 128 max cache size, 128 in cache
```

There is no workaround.

- CSCdv62884

  A Cisco 7500 series router with a multichannel E1 or T1 interface may reload unexpectedly if distributed IP header compression is enabled on the multichannel E1 or T1 interface.

  Workaround: Use the **no ip route-cache** interface configuration command to disable the distributed IP header compression function on the multichannel E1 or T1 interface.

- CSCdv63941

  A Cisco 7200VXR router with a Network Services Engine (NSE-1) may display incorrect NetFlow statistics after NetFlow is enabled.

  Workaround: Disable Parallel Express Forwarding (PXF) using the **no ip pxf** global configuration command.

- CSCdv65014

  Symptoms Digital signal processors (DSPs) may pause indefinitely on the originating end of a Cisco AS5300 that is receiving ISDN overlap calls.

  Conditions This symptom is observed when there are no dial peer matches for the calls.

  Workaround There is no workaround.

- CSCdv66641

  Symptoms Nongrouped ATM interfaces go down when an inverse multiplexing over ATM (IMA) group interface comes up. This situation prevents you from using multiple IMA groups or IMA interfaces and non-IMA interfaces simultaneously.

  Conditions This symptom is observed when the following sequence of events occurs:

  a. Configure all ports of an ATM module as nongrouped ATM interfaces.
  b. Enter the **no shutdown** interface configuration command on all interfaces to ensure that they reach the Up/Up state.
  c. On both routers of the ATM link, configure two of the ATM interfaces to become part of an IMA group.

  When the IMA group interface comes up, the two interfaces that have been configured to be part of the IMA group are up, but the remaining ungrouped ATM interfaces go down.

  Workaround Configure all interfaces of the ATM module to be part of a single IMA group.

- CSCdv67410

  Symptoms On a Cisco 7200VXR router that is using any unchannelized serial port adapter (PA) and any processor other than the Network Processing Engine (NPE-300), line flaps may occur at high traffic rates and the router may display the following message:

  ```
  MUESLIX-1-HALT: Mx serial: Serial6/0 TPU halted: cause 0x3 status 0x00371A00
  ```

  Carrier transitions and wedged output queues may also occur.

  Conditions This symptom is observed when you use any of the following port adapters:

  – PA-T3
  – PA-2T3

  - PA-T3+
  - PA-2T3+

  Multichannel port adapters such as the PA-MC-T3 or the PA-MC-2T3+ are not affected. This condition affects only the Cisco 7200VXR router.

  Workaround There is no workaround.

- CSCdv69663

  An Integrated Service Adapter (ISA) card that is running Cisco IOS Release 12.2 may lock up when a microcode reload is performed.

  Workaround: Reload the router if the microcode needs to be reloaded.

- CSCdv71496

  A Cisco 1710 router that is running Cisco IOS Release 12.2(2)XH may experience intermittent hanging of the LAN-to-LAN tunnel if both LAN-to-LAN and client access are configured. LAN-to-LAN will stop after remaining up for about a day. The router must be reloaded to reestablish the tunnel. There is no workaround.

- CSCdv72539

  Symptoms An ISDN rotary configuration with service policies attached does not classify packets and apply features correctly.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround Use a dialer profile configuration instead of a rotary configuration. If you cannot use a dialer profile configuration, there is no workaround.

- CSCdv73877

  Symptoms Traffic that is sent from a Multiprotocol Label Switching (MPLS) customer edge (CE) router (MPLS CE 1) to an MPLS CE router (MPLS CE 3) through two MPLS provider edge (PE) routers (MPLS PE 1 and MPLS PE 2) and an MPLS core is not accounted for properly with NetFlow on the incoming interface of the MPLS PE 1 router.

  Traffic is accounted for properly with NetFlow when traffic is sent from the MPLS CE 1 router to an MPLS CE router (MPLS CE 2) that is connected directly to the MPLS CE 1 router without going through the MPLS core.

  Conditions This symptom is observed on a Cisco 3640 router that is running Cisco IOS Release 12.1(5)T10 or Release 12.2(5a) and occurs only if the incoming interface runs Cisco Express Forwarding (CEF); it does not occur if the traffic that is arriving on an interface is configured to perform fast switching using the **no ip route-cache cef** command. The symptom does not affect the MPLS NetFlow egress functionality.

  This symptom is also observed on a Cisco 7500 series router that is running Cisco IOS Release 12.0.(19)S1 and that has distributed Cisco Express Forwarding (dCEF) enabled. In this case, the symptom is seen without Virtual Private Network routing and forwarding (VRF) instances and with any traffic that is coming in through a CEF-enabled interface and that needs to be MPLS-encapsulated to go into the MPLS core.

  Workaround Disable CEF.

- CSCdv77429

  A Cisco AS5800 universal access server that is running Cisco IOS Release 12.2(5.8a) may reload when ISDN PRI is configured simultaneously on several T1 controllers using a text file. This condition does not occur if the T1 controllers are configured individually.

Workaround: Avoid configuring ISDN PRI on several T1 controllers at one time. Configure ISDN PRI on each T1 controller individually.

- CSCdv78596

  Symptoms Outgoing packets may drop from a cable interface.

  Conditions This symptom is observed on a Cisco uBR7200 series router that is running Cisco IOS Release 12.1(9)EC and that has Cisco Express Forwarding (CEF) enabled.

  Workaround Disable and then reenable CEF.

- CSCdv79980

  Significant throughput degradation may occur on a PPP multilink if the fragment delay on a 2-port multichannel E1 port adapter (PA-MC-2E1) that is configured for channel groups is set to a value that is lower than the default value. There is no workaround.

- CSCdv80116

  Symptoms A cable modem does not function when baseline privacy interface (BPI) is enabled.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround Disable BPI.

- CSCdv80428

  A Cisco router may pause indefinitely when a virtual circuit (VC) class is attached to an interface that has a large number of VCs configured. When the router pauses indefinitely and if the adjacent interface and the local interface are shut down, the **show interface atm** EXEC command will indicate a negative number. After this error occurs, no more VCs can be created. To recover from this error, a user has to reboot the router.

  Workaround: To prevent this condition from occurring, do not shut down the adjacent interface in the middle of a VC class configuration.

- CSCdv80722

  Symptoms When you configure R2 signaling using the **ds0-group** controller configuration command, and before any calls are made, the status shows “seized” instead of “idle.”

  Conditions This symptom is observed on an E1 connection between two Cisco 3640 routers that are connected back to back.

  Workaround Enter the **ds0 busyout** controller configuration command.

- CSCdv81177

  A Cisco 7200 router may repeatedly display the following message when voice calls are present:

  ```
  %SYS-3-MGDTIMER: Timer has parent, timer link, timer = 623B6970. -Process=
  "CC-API_VCM", ipl= 4, pid= 112:
  ```

  These messages are harmless and do not affect the voice quality or the completion of the call.

  Workaround: Use a Cisco IOS release earlier than Cisco IOS Release 12.2(7).

- CSCdv83827

  Symptoms Explicit null labels may disappear from a Tag Forwarding Information Base (TFIB) after you enter the **no tag ip** global configuration command followed by the **tag ip** global configuration command.

  Conditions This symptom is observed when you configure the Label Distribution Protocol (LDP)/Tag Distribution Protocol (TDP) on a one-hop tunnel and also on a physical link between two label switching routers

Workaround Enter the **clear ip route** *ip-address* command, in which the *ip-address* argument is the IP address of the TFIB entry with the explicit null labels that disappeared.

- CSCdv83875

  Symptoms A router may stop sending traffic if the microcode is reloaded while the router is forwarding traffic.

  Conditions This symptom is observed on a Cisco 7500 series Versatile Interface Processor 4 (VIP4) that is configured with a 2-port Fast Ethernet port adapter (PA-2FE). This symptom can be resolved temporarily by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the PA-2FE interface.

  Workaround Reload the microcode while there is no egress traffic on the router.

- CSCdv88067

  On a device that is used as a Label Switch Controller (LSC) to control extended tag (XTAG) ATM interfaces, it is possible for the virtual switch interface (VSI) on the LSC to become out of synchronization with the VSI slave that is running on the controlled ATM switch.

  The following are symptoms that this condition occurring:

  - Tag virtual circuits (TVCs) fail to be created and virtual path identifier (VPI)/virtual circuit identifier (VCI) are reported as already in use.
  - Negative acknowledgment (NAK) errors are received from the slave.
  - The Tag Distribution Protocol (TDP) or Label Distribution Protocol (LDP) are not ready.

  To confirm if the VSI master and slave are out of synchronization, compare the number of TVCs that are seen by the LSC to the number of TVCs that are on the switch.

  Workaround: This caveat entry creates a new functionality for an existing command-line interface (CLI) command to initiate a resynchronization between a VSI master and a slave. The resynchronization can be initiated by issuing the **clear interface xtagatm** *number* command to clean up the stray connections on the ATM switch.

- CSCdv89201

  Symptoms When a permanent virtual circuit (PVC) changes from a state of no congestion to a state of congestion, Multilink PPP (MLP) fragments are dropped or received out of order at the remote end. The output of the **show ppp multilink** EXEC command displays the following:

```
Virtual-Access4, bundle name is xyz
   Bundle up for 03:56:11
   2524 lost fragments, 3786 reordered, 0 unassigned
   1262 discarded, 1262 lost received, 1/255 load
   0x42EA1 received sequence, 0xCF7 sent sequence
   Member links: 1 (max not set, min not set)
      Virtual-Access1, since 03:59:02, last rcvd seq 042EA0 400 weight
```

  Errors are also displayed in the output of the **debug ppp multilink events** EXEC command:

```
Vi4 MLP: Lost fragment 3FED9 in 'dhartr21' (all links have rcvd higher seq#)
Vi4 MLP: Received lost fragment seq 3FED9, expecting 3FEDC in 'dhartr21'
Vi4 MLP: Out of sync with peer, resyncing to last rcvd seq# (03FED9)
Vi4 MLP: Unusual jump in seq number, from 03FEDC to 03FEDA
```

  The condition is more evident with a higher "tx-ring-limit" value.

  Conditions This symptom is observed on a Cisco 3660 router that is running Cisco IOS Release 12.2(6.3)T and that is configured for MLP over ATM (MLPoATM) and class-based weighted fair queueing (CBWFQ)/low latency queueing (LLQ).

  Workaround There is no workaround.

- CSCdv90443

  Symptoms High memory utilization that results in malloc failures may occur on a router.

  Conditions This symptom is observed if you use the **ip route** *network-number network-mask ethernet [bay] slot/port* EXEC command to configure static routes to a prefix on a Cisco router that is capable of distributed Multiprotocol Label Switching (MPLS) forwarding (such as a Cisco 7500 series router or a Cisco 12000 series router). If you enter the **show cef linecard internal** command, many interprocess communication (IPC) messages appear to be queued up under the category "rtc."

  Workaround When a route is configured using the **ip route** *network-number network-mask ethernet [bay] slot/port* EXEC command, make sure that you also provide a next hop IP address. Use the following command to configure a next hop IP address: **ip route** *network-number network-mask ip-address ethernet [bay] slot/port* (where IP address is the next hop IP.)

- CSCdv90902

  On a Cisco router that is running Cisco IOS Release 12.0(19.3)ST2 through 12.0(19.6)ST or Release 12.2(6.4) through 12.2(7) and that is running Multiprotocol Label Switching (MPLS) Traffic Engineering (TE), the link management module may fail to advertise an administrative metric for an advertised link.

  This condition may occur on any MPLS TE interface that is not a subinterface. This condition occurs if the interface is explicitly configured in NVRAM and is administratively disabled using the **shutdown** interface configuration command. This condition may also occur if the interface is not configured at all in the NVRAM configuration because the device setup will automatically place the interface in the shutdown state. When the interface is subsequently administratively enabled, it may be flooded by the link management module without an administrative metric.

  This condition will not occur if a user-specified administrative weight is configured on the interface using the **mpls traffic-eng administrative-weight** interface configuration command.

  Workaround: After the interface is administratively enabled using the **no shutdown** interface configuration command, this condition can be corrected by performing either of the following steps:

  a. Disable and reenable MPLS TE on the interface using the **no mpls traffic-eng tunnels** interface configuration command followed by the **mpls traffic-eng tunnels** interface configuration command.

  b. Enable and disable a user-specified administrative weight by issuing the **mpls traffic-eng administrative-weight 10** interface configuration command followed by the **no mpls traffic-eng administrative-weight** interface configuration command.

- CSCdv90929

  A T1 controller that has Extended Superframe (ESF) framing may process an in-band channel service unit (CSU) remote loopback command with a facility data link (FDL) American National Standards Institute (ANSI) setting. There is no workaround.

- CSCdv91266

  In a Multiprotocol Label Switching (MPLS) over routed bridge encapsulation (RBE) environment, tagged packets are sent out as routed packets instead of bridged packets. MPLS support is needed for RBE interfaces. There is no workaround.

- CSCdw00005

  Symptoms Certain interfaces that are configured on a T1 line may stop passing traffic.

  Conditions This symptom is observed when a channelized port adapter (CT3) is used and if framing is reconfigured with the **t1 1 framing esf** privileged EXEC command. This condition occurs only if the **t1 1 framing esf** privileged EXEC command is issued after channel groups are already

configured on the T1 line and while the channel groups are passing traffic. The framing needs to be set only for the T1 line when the first channel group is configured and does not need to be reentered when a new channel group is added.

Workaround Issue the **t1 1 framing esf** privileged EXEC command only when the first interface on a T1 line is configured.

- CSCdw00011

  Symptoms All interfaces may stop passing traffic if T1 frames are received on one of the groups that has voice signaling enabled.

  Conditions This symptom is observed when a channelized T3 port adapter (CT3) that is configured with multiple channel groups is used.

  Workaround Shut down the interface that corresponds to the channel group that is receiving the invalid frame. If any of the other interfaces continues to flap after the interface that is receiving the invalid frame is shut down, the interface has to be reconfigured.

- CSCdw00013

  A Cisco 6340 router that is configured for R2 channel-associated signaling (CAS) may not play busy tones properly. There is no workaround.

- CSCdw00333

  Symptoms A service policy is not applied to a Fast Ethernet interface after the configuration is saved to NVRAM and after a router is reloaded.

  Conditions This symptom is observed on a Cisco 2600 series router that is running Cisco IOS Release 12.2(5) and on a Cisco 1700 series router that is running Cisco IOS Release 12.2(4)T.

  Workaround There is no workaround.

- CSCdw01193

  Symptoms A 99-percent CPU utilization condition may occur on a Cisco router.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.1(8).

  Workaround There is no workaround.

- CSCdw02485

  A FlexWAN module may reload when a distributed Multilink PPP (dMLP) 8-port channelized T1 port adapter (the second interface in a bundle) is configured using the encapsulation encapsulation-type interface configuration command.

  Workaround: Reload the FlexWAN module. After the FlexWAN module is reloaded, the configuration will be completed and the bundle should be active.

- CSCdw03257

  Symptoms An outgoing recEive and transMit (E&M) immediate-start voice call setup may fail because the terminating side misses one or more digits of the called number.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw04036

  Symptoms The following error message may be generated on a Cisco 7200VXR router:

  ```
  CRYPTO_ENGINE: locally-sourced pkt w/DF bit set is too big,ip->tl=1492, mtu=1418
  %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=62C93A40, count=0
  -Traceback= 605A305C 617A3D1C 6174DA78 6174E65C 606FF44C 606FE5E0 606FE988 6070B778
  6 06CC5BC 606D5184 606D494C 607B2084 607B2BB4 607 B2E1C 605E2E7C 605E2E68
  ```

Conditions This symptom is observed on a Cisco 7200VXR router that is configured with data-link switching (DLSw) and IP Security (IPSec) with the **tcp path mtu discovery** global configuration command enabled.

Workaround There is no workaround.

- CSCdw04099

  On a Cisco 10000 series edge services router that is configured for Border Gateway Protocol (BGP) traffic, if the **as-override** command is enabled for a peer group and if members are later added to that peer group, the **as-override** command does not take effect for the new members.

  Workaround: Disable and then reenable the **as-override** command for the peer group.

  Alternate workaround: Enable the **as-override** command individually for each member of the peer group.

- CSCdw04194

  If the IP maximum transmission unit (MTU) on a point-to-point interface changes while there are multiple adjacencies (of different link types) on an interface, only one adjacency will have the correct MTU configured. There is no workaround.

- CSCdw04473

  Symptoms A dial shelf controller (DSC) card may reload after the **dir slot0:** or **show slot0:** command is entered after a Personal Computer Memory Card International Association (PCMCIA) card is removed and reinserted.

  Conditions This symptom is observed in Cisco IOS Release 12.2(1)XS1 and Release 12.2(6).

  Workaround There is no workaround.

- CSCdw04669

  Symptoms A Cisco router reloads if the encapsulation is changed from PPP to High-Level Data Link Control (HDLC).

  Conditions This symptom is observed on a Packet-over-SONET interface that has the **mpls traffic-eng autoroute** command enabled and for which the autorouting first has occurred and then has cleared.

  Workaround There is no workaround.

- CSCdw05149

  Symptoms Calls that do not have a dial peer match are dropped before translation instead of being matched to an outgoing dial peer.

  Conditions This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(2)XB.

  Workaround Create a pseudo Voice over IP (VoIP) dial peer that has the proper destination pattern using a false session target.

- CSCdw05692

  Symptoms Security association (SA) connection are not established because the maximum transmission unit (MTU) path of the router peer is negative.

  Conditions This symptom is observed on an interface of a Cisco 1700 series router after the router reloads.

  Workaround Reapply the crypto map on the interface that is affected.

- CSCdw05710

  An ATM permanent virtual connection (PVC) may become inactive on a Node Route Processor (NRP) and display the following error message:

  ```
  %ATMCES-1-ERRCREATEVC: The 1575 device failed to create VC 6, line:1081
  ```

  Workaround: Reload the NRP.

- CSCdw05826

  Symptoms A Cisco 1720 router may reload with a segmentation violation (SegV) exception.

  Conditions This symptom is observed on a Cisco 1720 router that is running the c1700-ny-m image of Cisco IOS Release 12.1(4).

  Workaround There is no workaround.

- CSCdw05883

  Symptoms A Cisco 7204VXR router may reload because of a software condition.

  Conditions This symptom is observed on a Cisco 7204VXR router that is running the c7200-a3js-mz image of Cisco IOS Release 12.2(5a).

  Workaround There is no workaround.

- CSCdw06038

  Symptoms A customer profile may not be found for a particular dialed number identification service (DNIS) group. Calls that are coming in to an access server may not be able to access the customer profile, depending on the order, size, and value of the DNIS information that was entered, and depending on whether the DNIS information was manually entered or set up through the startup configuration when the access server reloaded.

  Conditions This symptom is observed on an access server that has resource pooling and authentication, authorization, and accounting (AAA) accounting configured.

  Workaround There is no workaround.

- CSCdw06963

  Symptoms Alignment error corrections at the rsp_ipfib_feature_switch process may occur on a Route Switch Module (RSM).

  Conditions This symptom is observed on an RSM that is running Cisco IOS Release 12.0(20) that has IP Cisco Express Forwarding (CEF) enabled.

  Workaround To clear the condition, disable IP CEF and use fast switching instead.

- CSCdw07767

  Time-division multiplexing (TDM) leaks when it is tested for hairpinning on a Cisco AS5850 access sever. This behavior affects only T1 channel-associated signaling (CAS) interfaces and not PRIs. There is no workaround.

- CSCdw09507

  Symptoms If a router sends an “Alert” message without a progress indicator (PI), a dial tone is heard instead of a ringback tone.

  Conditions This symptom is observed on a terminating router that is running Cisco IOS Release 12.2(6) and that is configured for ISDN or Signaling System 7 (SS7).

  Workaround Configure the terminating router to always send a PI with an “Alert” message. If “CC_PROG_INBAND” information (with a PI value of 8) is sent in the “Alert” message, a ringback will be received. Configure the **progress_ind alert enable 8** dial peer configuration command on the outgoing plain old telephone service (POTS) dial peer of the terminating router.

- CSCdw09521

  A Cisco 7500 router that is running Cisco IOS Release 12.2(6.3) may experience a reload of the Versatile Interface Processor (VIP) if a service policy is attached to an inverse multiplexing over ATM (IMA) interface. There is no workaround.

- CSCdw09736

  Symptoms When the Generic Transparent Descriptor (GTD) is enabled with "gtdparamstring=ALL" on a Public Switched Telephone Network (PSTN) Gateway 2000 (PGW 2200), GTD data is sent in two segments. The segments should be combined in a "SetUp" message, but the combining process does not work properly and causes the "SetUp" message to fail with an invalid setup message (cause code 61) for every other call.

  Conditions This symptom is observed on switched calls that are made in a PRI to ISDN User Part (ISUP) time-division multiplexing (TDM) configuration.

  Workaround There is no workaround.

- CSCdw10010

  Symptoms A router may not forward multicast traffic over a PA-2FE port channel in a distributed path.

  Conditions This symptom is observed on a Cisco 7504 router that is running Cisco IOS Release 12.2(6.3)T. The multicast traffic is switched in the fast-switching path only. Caveat CSCds38187 has fixed this condition for the 1-port PA-FE port adapter.

  Workaround There is no workaround.

- CSCdw10550

  On an interface of a Cisco 7500 series router, if the input service policies have the same classes as the output service policies and if an invalid configuration is created by attaching an input service policy with the same queuing feature that is already enabled on the output service policy, the input service policy will be denied. If the output service policy is updated, the router may reload.

  Workaround: First remove the output service policy from the interface and then reconfigure and update the output service policy.

- CSCdw11002

  A Cisco router may reload if the **ip address dhcp** command, the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command are entered in quick succession on an Ethernet or a Fast Ethernet interface. This condition occurs when there is no Dynamic Host Configuration Protocol (DHCP) server running. There is no workaround.

- CSCdw11263

  Symptoms When you reload a Cisco 7200 series router with bidirectional traffic enabled, the router may reload at dec21140_rx_interrupt. The router does not reload after a successful bootup or during normal operation.

  Conditions This symptom is observed on a Cisco 7200 series router that is configured as a Layer 2 Tunneling Protocol (L2TP) Network Server (LNS).

  Workaround Reload the router with low traffic or no traffic at all.

- CSCdw13432

  When the called party is busy in a two-stage call scenario, the calling party may not hear a busy tone and the call terminates immediately. This behavior is observed with Cisco IOS Release 12.2(2)XB, Release 12.2(7), and some earlier 12.2 releases. There is no workaround.

- CSCdw13574

  Symptoms An ATM Circuit Emulation Services (CES) port adapter (PA-A2) may receive output drops when the peak cell rate (PCR) is reached. Output drops continue to occur on the interface, even after the traffic flow is stopped. The output drops stop after you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface.

  Conditions This symptom is observed when more than one permanent virtual connection (PVC) is configured.

  Workaround There is no workaround.

- CSCdw14254

  Symptoms ISDN interfaces are not usable because the **isdn spid** interface configuration command that assigns service profile identifiers (SPIDs) for the channels is not accepted. When this behavior occurs, the interface cannot communicate properly with ISDN switches.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw14262

  Symptoms On a Cisco Voice over IP (VoIP) gateway, a high CPU memory utilization condition may occur at the CCH323_CT process.

  Conditions This symptom is observed on a VoIP gateway that is running a Cisco IOS Release 12.2(1a) IP plus image.

  Workaround There is no workaround.

- CSCdw14673

  A Cisco router that is running Cisco IOS Release 12.2 T may experience a software-forced reload when it is configured as an H.323 gatekeeper. There is no workaround.

- CSCdw16581

  Symptoms Cisco IOS software does not send attribute 30 (called numbers) to a RADIUS server when it is authenticating the remote username. If a Modem ISDN channel aggregation (MICA) technologies card is used, the attribute is sent in the authentication access request.

  Conditions This symptom is observed when large scale dialout (LSDO) is used on a Cisco 3640 router that is running Cisco IOS Release 12.2(6.4) and when the NM-8AM or NM-16AM network module analog modems are used

  Workaround There is no workaround.

- CSCdw16685

  Symptoms Packets that are forwarded through the interface are punted to the process switch layer.

  Conditions This symptom is observed when there are no Forwarding Information Base (FIB) entries for routes via a generic routing encapsulation (GRE) tunnel that uses policy routing to set the default interface to the GRE tunnel. The occurrence of this behavior can be confirmed by examining the switching statistics on the interface using the **show interface statistics** EXEC command. This behavior occurs because Cisco Express Forwarding (CEF) does not have adjacency information for the tunnel interface.

  Workaround Add a static route that points out the GRE tunnel to force CEF to add the adjacency.

- CSCdw16710

  Symptoms Real-Time Transport Protocol (RTP) header compression becomes inactive on a Frame Relay subinterface.

  Conditions This symptom is observed after a header compression instance is deleted using the **no frame-relay ip rtp header-compression** interface configuration command while fast switching is used with IP header compression.

  Workaround Reenable header compression on the subinterface using the **frame-relay ip rtp header-compression** interface configuration command.

- CSCdw16903

  Symptoms When routing traffic is sent between PRI/ISDN and H.323 Voice over IP (VoIP) network legs, a memory leak may occur and the router may reload.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(7) or an earlier release. The symptom occurs when the router is handling the pass-through of Q Signaling (QSIG) messages from an ISDN call leg through a VoIP network. The memory leakage occurs when H.225 connection timeouts occur on the VoIP call legs. To determine if this condition is occurring, enter the **show h323 gateway h225** privileged EXEC command. If the symptom is occurring, a positive value is displayed for the "H.225 establish timeout" statistic. This leak will not occur when normal voice call traffic is handled.

  The number of timeouts can be reduced and the memory leak can be minimized by increasing the H.323 connection timeout value. The H.323 connection timeout value can be adjusted by issuing the **voice class h323** *tag* global configuration command. The adjusted value must subsequently be associated with the voice dial peers. The default value is 15 seconds and can be increased to a maximum of 30 seconds.

  Workaround There is no workaround.

- CSCdw17073

  Symptoms On a platform that is configured with an active and a standby home agent (HA), continuous debugs appear on both HAs.

  Conditions This symptom is observed after the following sequence of event has occurred:

  a. Send a registration request so that bindings are created on both the active and the standby HA.
  b. Clear the bindings on the standby HA by entering the **clear ip mobile binding all** EXEC command on both HAs.
  c. Turn on the following debug commands on both HAs: the **debug ip mobile** EXEC command and the **debug ip mobile standby** EXEC command.
  d. Increase the standby priority by entering the **standby priority 150** interface configuration command so that it becomes active.

  Workaround Turn off the debug commands.

- CSCdw17131

  Symptoms When a Toolkit Command Language (TCL) interactive voice response (IVR) 2.0 script that uses the blast call function is used to initiate multiple outbound calls, some call legs may not be properly torn down after the call completes.

  Conditions This symptom is observed when the TCL IVR 2.0 script that is running on the gateway uses the blast call function to place simultaneous calls to multiple destinations.

  Workaround Modify the TCL IVR script to place calls sequentially instead of using the blast call function.

- CSCdw18116

  Symptoms An output stuck condition may occur on a multichannel port adapter such as a PA-MC-T1 or a PA-MC-E1.

  Conditions This symptom is observed under stress conditions when the port adapter is configured to operate in the PRI mode.

  For further information about "output stuck" messages that are reported on a Route Switch Processor (RSP), refer to the "What Causes %RSP-3-RESTART: interface [xxx], output stuck/frozen/not transmitting Messages?" section of the Cisco documentation at the following location:

  http://www.cisco.com/warp/public/63/output_stuck.shtml

  Workaround There is no workaround.

- CSCdw18196

  Symptoms Packets that are process switched to an ATM permanent virtual connection (PVC) may undergo incorrect policing. The policer configuration includes one or more actions that contain the "set-clp-transmit" process, but the ATM cells that are generated by the packets do not have a Cell Loss Priority (CLP) bit set.

  Conditions This symptom is observed only when packets that are process switched undergo policing.

  Workaround There is no workaround.

- CSCdw18282

  A basic call cannot be established if a voice port is configured with a multifrequency (MF) tone dial type and the incoming plain old telephone service (POTS) dial peer uses the interactive voice response (IVR) 2.0 application "session" which cannot process MF digits, particularly digits such as KP and ST. There is no workaround.

- CSCdw18371

  Symptoms A Cisco router that is running Resource Reservation Protocol (RSVP) over ATM may reload at the rsp_ipfib_feature_switch process while data traffic is traveling over switched virtual circuits (SVCs) that are established by RSVP. The router reloads after the **no ip cef** global configuration command and the **ip cef** global configuration command are issued in succession.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.1 T, Release 12.2, or Release 12.2 T and that has RSVP over ATM reservations.

  Workaround Unconfigure Cisco Express Forwarding (CEF) by removing the RSVP configuration from all ATM interfaces using the **no ip rsvp bandwidth** interface configuration command. Then reenable CEF using the **ip cef** global configuration command, the **ip rsvp bandwidth** interface configuration command, and the **ip rsvp svc-required** interface configuration command.

- CSCdw18482

  Symptoms When a vendor-specific Mobile Station (MS) talks to a Cisco gateway general packet radio service (GPRS) support node (GGSN), the MS may send the "IP Header Compression" IP Control Protocol (IPCP) option when it is activating the Protocol Data Packet (PDP) context. Cisco GGSN will always reject this PDP context request because this option is not supported by GGSN.

  Cisco GGSN should instead accept this PDP context request (if authentication and other configurations are successful) and reject the IPCP option. The idea is to allow GGSN to reject IP header compression but not reject the PDP context. GGSN should reject any unsupported IPCP option but GGSN should allow the PDP context to go through if authentication is successful.

  Conditions The conditions under which this symptom occurs are not known at this time.

Workaround There is no workaround.

- CSCdw18697

  Symptoms A Cisco router may pause indefinitely when network-based application recognition (NBAR) is enabled.

  Conditions This symptom is observed on a Cisco 7200 series and Cisco 7500 series router.

  Workaround Use the **ip nbar resources** *max-age initial-links expand-links* global configuration command.

  For example, if the **ip nbar resources 600** *initial-links* **50** global configuration command is issued, the system will wait for 600 seconds (10 minutes) before it tries to clean up a flow.

  Note According to what the system will allow, use the maximum amount for the *initial-links* argument to specify the number of preallocation links that the resource manager should preallocate at initialization time.

- CSCdw18763

  Symptoms PPP multilink is not able to reassemble received packets that have more than 16 multilink fragments.

  Conditions This symptom is observed when PPP multilink is used on Cisco 1700 series routers.

  Workaround There is no workaround.

- CSCdw18876

  Symptoms Common channel signaling (CCS) over ATM adaptation layer 5 (AAL5) does not work on a router that is running Cisco IOS Release 12.2 T when a high density voice network module (NM-HDV) is used. The ISDN layer does not come up. There is no workaround.

- CSCdw19011

  Symptoms A serial port adapter (PA-2E3) may exhibit cyclic redundancy check (CRC) errors.

  Conditions This symptom is observed when a PA-2E3 is connected to a vendor-specific device using a shorter cable

  Workaround There is no workaround.

- CSCdw19358

  Symptoms Passive FTP transfers with Context-Based Access Control (CBAC) may be refused.

  Conditions This symptom is observed when certain FTP servers are used.

  Workaround There is no workaround.

- CSCdw19436

  Symptoms If a setup message is received with no called and calling party number, an access server reloads.

  Conditions This symptom is observed on ISDN interfaces.

  Workaround There is no workaround.

- CSCdw19677

  Symptoms A Cisco Router Route Processor (Gigabit Route Processor [GRP], Route Switch Processor [RSP], or Network Processing Engine [NPE]) may reload.

Conditions This symptom is observed when a traffic engineering (TE) tunnel interface is disabled and reenabled immediately using the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

The router may also exhibit this behavior either when tag switching is enabled and disabled using the **no tag-switching ip** interface configuration command followed in quick succession by the **tag-switching ip** interface configuration command or when a loopback interface is disabled and reenabled using the **shutdown** interface configuration command followed immediately by the **no shutdown** interface configuration command.

This behavior may also occur when a file is copied to the running configuration to change the state of a tunnel.

Workaround Wait for at least a minute after the **shutdown** interface configuration command is issued before entering the **no shutdown** interface configuration command on a tunnel interface or its associated loopback interface.

Wait for at least a minute after the **no tag-switching ip** interface configuration command is issued before entering the **tag-switching ip** interface configuration command.

Shut down all tunnel interfaces before copying a file to the running configuration.

- CSCdw20118

  Symptoms The **copy rcp** *device:filename* **startup-config** privileged EXEC command may fail if the destination filename is specified.

  Conditions The behavior observed in this caveat may be similar to the behavior that is described in CSCdu24409.

  Workaround There is no workaround.

- CSCdw20152

  Symptoms A Cisco 7200 series router may reload.

  Conditions This symptom is observed when a switched virtual circuit (SVC) is configured on an ATM interface. The symptom may not be limited to the Cisco 7200 series router.

  Workaround There is no workaround.

- CSCdw20568

  The CISCO-CLASS_BASED-QOS MIB is not supported on a Route Processor Module (RPM) card. There is no workaround.

- CSCdw20801

  Symptoms The following error messages are displayed immediately after a Cisco 7200VXR router is reloaded:

  ```
  %SYS-2-INTSCHED: 'sleep for' at level 3 -Process= "Init", ipl= 3, pid= 2
  -Traceback= 6064AA94 60633C04 60FFD1C4 611867AC 6066D1CC 60596134 603D1EB0 603D30BC
  603C3110 603D1C20 603BCB30 601F2480 601F0460 601F09F0 601F0840 60599A60
  ```

  The **ip cef** global configuration command and the police settings are class-map configurations and need to have a packet identification mechanism before anything is policed (such as match protocol http). This condition does not occur until the policy map is attached to an interface.

  Conditions This symptom is observed after a Cisco 7200VXR router is reloaded after it had been configured with the following commands:

  ```
  ip cef
  policy-map test-policy
    class-map test-class
      match protocol http
      police cir 64000 bc 16000 pir 64000 be 16000
  ```

```
    conform-action set-clp-transmit
    exceed-action set-clp-transmit
    violate-action set-clp-transmit
interface e3/1
  service-policy input test-policy
```

Workaround Reboot the router and detach the service policy containing Network-Based Application Recognition (NBAR) from all interfaces. After the router has rebooted, reattach the service policy. Save a copy of configuration file with the service-policy that is detached from interface in case the router reboots inadvertently because of an accidental power failure.

- CSCdw20980

  Symptoms If there are static routes defined that use the interfaces on a failed Versatile Interface Processor (VIP), traffic that is using those static routes may fail. The static routes include those that are defined within a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) routing and forwarding (VRF) instance.

  Conditions This symptom is observed when you perform an online insertion and removal (OIR) of a Versatile Interface Processor (VIP) in a Cisco 7500 series router or use the Single Line Card Reload (SLCR) feature after a VIP has reloaded unexpectedly.

  Workaround Enter the **clear cef linecard** *slot-number* **adjacency** EXEC command on the affected VIP.

- CSCdw21652

  Symptoms When a quality of service (QoS) service policy that is configured with the **bandwidth** *bandwidth-kbps* command is attached to an ATM permanent virtual circuit (PVC), the following error message may be displayed:

  ```
  bandwidth assignment must be at least 1% of link rate
  ```

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround Use the **bandwidth percent** *percent* command instead.

- CSCdw22219

  If a Private Network-Network Interface (PNNI) receives a high rate of corrupted PNNI topology state packets (PTSPs) continuously over a long period of time, a large number of internal node numbers may be generated for bogus node identifications (IDs). A reload may also occur if the number of internal node numbers reaches 1032. Under normal conditions, there should be a low rate of corrupted PTSP packets. However, if a PNNI is tunneled through a network in which connections are rate limited to a rate that is too low, the rate limiting may cause cell drops, which may in turn cause corrupt packets.

  Workaround: Isolate and remove the cause of PTSP packet corruption.

- CSCdw22261

  Calls that are placed to toll-free numbers in Saudi Arabia and Venezuela are immediately disconnected. This condition affects R2 backward signaling in those countries. There is no workaround.

- CSCdw22639

  On a Cisco router that is running Cisco IOS Release 12.2(6), if security is configured on an H.323 gateway using the **security password** command, the command is deleted from the configuration after the router is reloaded. If the router is upgraded from Cisco IOS Release 12.1(5)T10 to 12.2(6), the **security password** command is changed to a different syntax format.

  Workaround: Unconfigure and reconfigure the **gateway** command and then reconfigure the **security password** command.

- CSCdw23087

  Symptoms During operation of a Cisco 7200 series Integrated Service Adapter (SA-ISA), various errors are reported by the SA-ISA: 1C08,1C39, and others. The microcode of the SA-ISA may pause indefinitely or fail.

  Conditions This symptom is observed during operation of the SA-ISA, and is caused by a problem during the build of the SA-ISA microcode when the new compiler version c2.95.3 is used. (For this problem not to occur, the SA-ISA microcode should be built with the compiler version 97r1-9804b.)

  Workaround Instead of an SA-ISA, use software encryption.

  Alternate Workaround Upgrade to a Cisco IOS software image in which the SA-ISA microcode has been built with compiler version 97r1-9804b, for example, Cisco IOS Release 12.1(10)E or Release 12.2(8)T.

- CSCdw23661

  Symptoms A Cisco 4224 router may not be able to place a fax call to a Cisco 2660 router over a 2-MB link. Calls are connected but no answering fax tone is heard, and after some idle time, the calling fax disconnects because it does detect a signal from the answering fax.

  Conditions This symptom is observed in the following topology:

  The public switched telephone network (PSTN) connects over an E1 link to the Cisco 4224 router that is connected to a Cisco 827 router, which, in turn, is connected over a 2-MB WAN link to a Foreign Exchange Station (FXS) voice/fax interface card that is installed in a Cisco 2660 router.

  Workaround There is no workaround.

- CSCdw23758

  Cisco routers that are running gateway images from Cisco IOS Release 12.2(6) or an earlier release and that are using gateway security may report an incorrect disconnect reason if a call is terminated because of network connectivity problems.

  When gateway security is enabled, a disengage request (DRQ) message that includes a billing token is sent to the gatekeeper when a call is terminated. The billing token includes a DISCONNECT REASON and DISCONNECT STRING. If a network error occurs while a call is active, such that the connection between the originating and terminating gateways is lost, the call is dropped and a DRQ is generated.

  Prior to Cisco IOS Release 12.2, this condition results in a DISCONNECT REASON of 2 and a DISCONNECT STRING of “no route to destination.” In Cisco IOS Release 12.2 and releases up to and including Release 12.2(6), this condition erroneously results in a DISCONNECT REASON of 0 and a DISCONNECT STRING of “normal call clearing.”

  There is no workaround.

- CSCdw23797

  Symptoms A Cisco AS5300 causes the clear_modem() to be called on the wrong voice device (VDEV).

  Conditions This symptom is observed when the **ds0 busyout** controller configuration command is entered on a time slot that has an active voice call using the Simple Network Management Protocol (SNMP) or the command-line interface (CLI).

  Workaround There is no workaround.

- CSCdw24225

  A communication server for S/390 (CS/390) may receive many transmission group (TG) updates and cause poor performance on the host. As a dependent logical unit requestor (DLUR), Systems Network Architectures Switching Services (SNASw) reports TG updates to the host dependent

logical unit server (DLUS). This is normal operation. However, SNASw is making several TG updates for one connection because the control point (CP) name is generated dynamically. All of the TGs have CP names that begin with "@C", and most of the TGs are in the INOP state. There is no workaround.

- CSCdw25047

  Symptoms A memory leak occurs on a router.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.1(8). The symptom occurs at the "logger" process. There is also increased utilization in the "tty background" process. This is seen when the **show process cpu** EXEC command is issued.

  Workaround Disable "logging synchronous" under the vty, aux, and console ports. For example, to disable "logging synchronous" under the console port, enter the **line configuration 0 no logging synchronous** command.

- CSCdw25090

  A Cisco 7500 router may reload because of a watchdog timeout. There is no workaround.

- CSCdw25143

  Symptoms The ATM permanent virtual connection (PVC) on a Cisco 1417 router may remain in the inactive state after the router boots up. Traffic will not be passed out to the ATM interface when this condition occurs.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround Enter the **no shutdown** interface configuration command on the ATM subinterface.

- CSCdw25191

  Symptoms A Cisco router may reload if the **no tag ip** global configuration command is entered after the router has rebooted.

  Conditions This symptom is observed when the **no tag ip** global configuration command is entered after thousands of tag bindings have been established for hundreds of destinations.

  Workaround Use the **no tag ip** interface configuration command on each interface instead of using the **no tag ip** global configuration command on the router.

- CSCdw25746

  Symptoms A Cisco voice gateway may reload during a high level of traffic.

  Conditions This symptom is observed in Cisco IOS Release 12.2(2)XB2 and Cisco IOS Release 12.2.

  Workaround There is no workaround.

- CSCdw26306

  Symptoms If the **write memory** EXEC command is issued simultaneously with the **show configuration** privileged EXEC command or the **show running-config** EXEC command via two individual Telnet sessions by two different users, output similar to the following may be displayed:

  ```
  bGc nx ^@^@^@^A^A^A^@^@^A^@^@^E^@^@^@^@^@^@^@^@^@^@^@^@^@^@^A^@^
  ```

  Conditions This symptom is observed on a Cisco 7500 router that is running Cisco IOS Release 12.1(10)E.

  Workaround There is no workaround.

- CSCdw26311

  Symptoms If an H.323 “release complete” message that contains a Progress Indicator (PI) is received by a gateway, the call is not torn down correctly if the call is a channel-associated signaling (CAS) call.

  Conditions This symptom is observed on a Cisco 3640 router in the following topology:

  A Cisco 3640 router is connected via a PRI link to a Cisco AS5350 that is connected via a voice over IP (VoIP) link to another Cisco AS5300 that is, in turn, connected over either a T1 CAS link or an E1 R2 link to another Cisco 3640 router.

  Workaround Configure the gateway to not send the PI in the H.323 “release complete” message via the following **disc_pi_off** voice-port configuration command-line interface (CLI) command under the voice port, as in the following example:

  ```
  r3640# configure terminal
  r3640(config)# voice-port 2/1:23
  r33640(config-voiceport)# disc_pi_off
  ```

- CSCdw26331

  Symptoms Calls may receive a “no route to destination” message and an incorrect clearing cause code (instead of a user busy cause code). Depending on the equipment that is used, the caller may receive a “number unobtainable” message or fast busy tones instead of a busy tone when this condition occurs.

  Conditions This symptom is observed when calls are placed to a Foreign Exchange Station (FXS) on a busy interface.

  Workaround Add a “huntstop” on the dial peer that is assigned to the FXS interface.

- CSCdw27412

  The configured controllers on a Cisco AS5800 universal access server may fail to come up. There is no workaround.

- CSCdw27574

  Symptoms The maximum digit length is reduced from 128 to 13 digits in a replacement pattern for translation rules.

  Conditions This symptom is observed in Cisco IOS Release 12.2(6.7).

  Workaround Split the translation and configure part of the translation on the inbound leg and the other half of the translation on the outbound leg.

- CSCdw27622

  When a downstream 2.0 device connects by using an exchange identification (XID) of 0, Systems Network Architectures Switching Services (SNASw) treats this connection as a 2.1-type connection and generates a transmission group (TG) update. Sometimes, a downlink type TG is identified as an uplink type TG and is reported to the dependent logical unit server (DLUS) using a topology database update (TDU). This behavior may result in an excessive number of TG records on the host (see CSCdw24225). All of the TGs have CP names that begin with “@C”, and most of the TGs are in the INOP state. There is no workaround.

- CSCdw27800

  Symptoms A Versatile Interface Processor (VIP) may reload.

  Conditions This symptom is observed when distributed Multilink PPP (dMLP) is configured on a channelized T3 or E3 interface after the router is reloaded and booted up.

  Workaround There is no workaround.

- CSCdw27936

  Symptoms A ping may not go through across ATM adaptation layer 5 (AAL5) Subnetwork Access Protocol (SNAP) encapsulated interfaces.

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(6.8)T.

  Workaround There is no workaround.

- CSCdw28317

  Symptoms A Cisco AS5300 may reload under moderate-to-heavy call volume with memory leak errors and may generate the following stack trace:

  ```
  System was restarted by error - a Software forced crash, PC 0x6039AE4C
  ```

  The memory leak occurs when the gatekeeper returns at least one alternate endpoint that contains clear tokens in the registration confirmation (RCF) and the gateway sends an H.225 setup message to an alternate destination after the primary destination fails.

  Conditions This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.2(2)XA3 and that is using 128 MB of DRAM.

  Workaround There is no workaround.

- CSCdw29011

  Symptoms A caller receives a Q.931 Disconnect message with a Normal Call clearing cause code instead of a user busy cause code. The caller will also not hear any tones.

  Conditions This symptom is observed when a caller is connected to the BRI port on a Cisco 2600 router calls a busy number (that is connected via the PRI port of a Cisco AS5300) via an H.323 network using gatekeepers. The caller receives a Q.931 Disconnect message with a Normal Call clearing cause code instead of a user busy cause code from the BRI port.

  Workaround There is no workaround.

- CSCdw29063

  Symptoms When the **clear ip bgp *** command is entered at the console, a bus error may occur on a router and the router may reload.

  Conditions This symptom is observed when a large number of routes have been imported.

  Workaround There is no workaround.

- CSCdw29595

  The performance of the encryption path degrades when Cisco IOS Release 12.2(6.8) is used with a hardware encryption card. The loss in performance occurs because encrypted packets are process-switched instead of being fast-switched. This condition occurs when IP Security (IPSec) is applied to the interfaces while the hardware encryption card is used. There is no workaround.

- CSCdw29751

  Symptoms The **format** EXEC command generates an error message during the formatting of a 32-MB, 48-MB, or 64-MB Personal Computer Memory Card International Association (PCMCIA) linear Flash card.

  Conditions This symptom is observed on a Cisco Catalyst 6000 series switch.

  Workaround Use a PCMCIA Flash card that has a capacity of less than 32 MB.

- CSCdw29890

  Symptoms The **tx-ring-limit** command-line interface (CLI) command does not have any effect on the members of a permanent virtual connection (PVC) bundle.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw29901

  Symptoms The **vc-hold-queue** interface configuration command cannot be used for ATM permanent virtual connection (PVC) bundles.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw30320

  Symptoms A forwarding table may not be populated with the complete Layer 2 outgoing information, and packet loss may occur.

  Conditions This symptom is observed on a Cisco 12000 series Internet router or a Cisco 10000 series edge services router in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) and Gigabit Ethernet environment.

  Workaround Enter the **clear ip route** EXEC command for the affected prefix.

- CSCdw31637

  Symptoms Misaligned or spurious memory accesses may be detected on a Versatile Interface Processor (VIP) at the hqf_get_policymap() process.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw32067

  Symptoms An access server shows that modems are in use when there are no active users connected.

  Conditions This symptom is observed on a Cisco AS5800 that is running Cisco IOS Release 12.1(11) and that has Resource Pool Management (RPM) or Resource Pool Manager Server (RPMS) enabled.

  Workaround There is no workaround.

- CSCdw32302

  In a setup in which Internetwork Packet Exchange (IPX) traffic is passed between a client and server on different token rings and if the token rings are put in a bridge group on a Cisco router that is performing integrated routing and bridging (IRB), the router bitswaps the source MAC address from the client before putting the source MAC address into ring number 2. This behavior causes the connection to fail. The connection comes up normally if both the client and the server are on the same ring and when none of configuration on the devices is changed. This behavior occurs only with MAC-level multicast or broadcast traffic (such as Routing Information Protocol [RIP] traffic). There is no workaround.

- CSCdw32708

  A Cisco 3660 router that is running E1 R2 signaling may intermittently experience voice ports that are stuck in the “clear backward” state. The ports lock up for 2 seconds to 30 minutes; three to twenty voice ports can be affected.

  When this condition occurs, the following command output is displayed if the **show voice port summary** EXEC command is issued:

```
3/0:1   15 r2-digital up    up   idle     answered y
3/0:1   17 r2-digital up    up   idle     clearbak y
3/0:1   18 r2-digital up    up   idle     clearbak y
3/0:1   19 r2-digital up    up   idle     clearbak y
3/0:1   20 r2-digital up    up   idle     answered y
```

There is no workaround.

- CSCdw32840

  System Network Architecture Switching Services (SNASw) intermediate session routing (ISR) sessions that have an enterprise extender (EE) upstream may have messages that are unnecessarily segmented. Messages may be segmented because the CAPACITY on the physical unit (PU) definition on the host is too low, or because the wrong primary send/recv basic transmission unit (BTU) size is being used by the SNASw router.

  Once the segmenting of messages starts to occur (for either of these above reasons), the End Of Message (EOM) segment may be corrupted, causing the other end of the Rapid Transport Protocol (RTP) connection to identify a gap and request the message to be rebroadcasted. This behavior can cause significant delays of up to 2 minutes before the gap detected status is returned to the SNASw router.

  Workaround: To prevent the segmenting from occurring, add CAPACITY=4M to the PU definition on the host.

- CSCdw33027

  While fixing vulnerabilities mentioned in the Cisco Security Advisory: Multiple SSH Vulnerabilities (http://www.cisco.com/warp/public/707/SSH-multiple-pub.html) we inadvertently introduced an instability in some products.

  When an attacker tries to exploit the vulnerability VU#945216 (described in the CERT/CC Vulnerability Note at http://www.kb.cert.org/vuls/id/945216) the SSH module will consume too much of the processor's time, effectively causing a DoS. In some cases the device will reboot. In order to be exposed SSH must be enabled on the device.

  Affected product lines are:

  - All devices running Cisco IOSÆ Software supporting SSH. This includes routers and switches running Cisco IOS Software.
  - Catalyst 6000 switches running CatOS.
  - Cisco PIX Firewall.
  - Cisco 11000 Content Service Switch family.

  No other Cisco product is vulnerable. It is possible to mitigate this vulnerability by preventing, or having control over, the SSH traffic.

  This advisory is available at http://www.cisco.com/warp/public/707/SSH-scanning.shtml.

- CSCdw34627

  Symptoms When Frame Relay Forum (FRF.12) is enabled, the default Weighted Random Early Detection (WRED) settings in a modular quality of service command-line interface (MQC) are different from when the service is not enabled. When FRF.12 is enabled, the defaults revert to the non-FRF.12 settings.

  Conditions This symptom is observed after a router is reloaded or when the WRED parameters are changed.

  Workaround Reload the router.

- CSCdw34831

  Symptoms The message "Failed to get packet buffer on DS" may be displayed continuously on a dial shelf. The CPU usage on the router shelf may reach 99 percent.

  Conditions This symptom is observed on a Cisco AS5800 image that is built from Cisco IOS Release 12.2 or Release 12.2 T.

  Workaround There is no workaround.

- CSCdw35829

  If a subinterface is configured under the Fast Ethernet interface of a Node Route Processor 1 (NRP-1) that is running Open Shortest Path First (OSPF), all the OSPF neighbors associated with the Fast Ethernet interface may be reset. There is no workaround.

- CSCdw36571

  Symptoms A router may reload when it generates a configuration.

  Conditions This symptom is observed on a router when it generates a configuration (such as when it executes the **show run** EXEC command, the **show tech** EXEC command, or the **write memory** privileged EXEC command). This symptom is observed when the router is configured to perform a large number of static Network Address Translations (NATs).

  Workaround There is no workaround.

- CSCdw37729

  Symptoms When a voice gateway sends an admission request (ARQ) to a voice gatekeeper (GK), the voice GK sends a location request (LRQ) to a second voice GK. The second voice GK sends the LRQ back to the first voice GK, in correspondence with the configuration. In response to this LRQ, an incorrect address resolution occurs on the first voice GK, and it sends a location confirmation (LCF) with its own registered default-technology gateway IP to the second voice GK.

  Conditions This symptom is observed on a Cisco 7200 series router that is functioning as a voice GK (that is, as the first voice GK in the symptom described) and that is running the c7200-jx2-mz image of Cisco IOS Release 12.2(2)T when it communicates with another voice GK (that is, the second voice GK in the symptom described) and when these two voice GKs are misconfigured to send the same LRQ back and forth.

  Workaround There is no workaround.

- CSCdw37797

  Symptoms Connection trunks fail.

  Conditions This symptom is observed when a router is configured with connection trunks that connect DS0 groups on the same controller or with connection trunks on the same voice WAN interface cards (VWIC) or WAN interface cards (WIC) in a slot.

  Workaround Reconfigure the connection trunks so that they do not connect between DS0 groups that reside on the same controller.

- CSCdw37839

  Symptoms A Cisco AS5400 does not send a Simple Network Management Protocol (SNMP) LinkUp trap when the cable of an E1 controller is plugged into the Cisco AS5400, which is incorrect behavior.

  Conditions This symptom is observed on a Cisco AS5400 that is running Cisco IOS Release 12.2(2)XB1 after the cable of the E1 controller is first unplugged and then plugged in again. Note that when the cable of the E1 controller is unplugged, the Cisco AS5400 does send an SNMP LinkDown trap, which is correct behavior.

Workaround There is no workaround.

- CSCdw37864

  Symptoms An originating gatekeeper does not recognize and use a modified destination call signal address from a location confirmation (LCF) response in its admission confirm (ACF) reply to an originating gateway.

  Conditions This symptom is observed when an H.323 Voice over IP (VoIP) call signaling flow that is manipulated via Gatekeeper Transaction Message Protocol (GKTMP) is routed from an originating gateway to an originating gatekeeper, then to a terminating gatekeeper, and finally to a terminating gateway.

  Workaround There is no workaround.

- CSCdw38373

  Symptoms A clear to send (CTS) signal on a port is inverted for a short period of time when binary synchronous communication (BISYNC) polling is started after a router is reloaded. This behavior causes an ATM platform to enter the error recovery mode and may prevent the ATM platform from recovering and reestablishing proper communication with the router.

  Conditions These symptoms are observed on a Cisco 2600 series router that is configured with a 2-port serial low-speed asynchronous and synchronous WAN interface card (WIC-2-A/S) that is configured for BISYNC on one port (port 0) and that has the **physical-layer async** interface configuration command configured on the other port (port 1).

  Workaround After you have initialized the ports through reloading the WIC or after the **physical-layer async** interface configuration command has been removed from the configuration of a port, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the serial interface to reinitialize the hardware settings.

- CSCdw38440

  Symptoms On a Cisco 7200 series router, the time taken for 250 simultaneous Internet Key Exchange (IKE) sessions to come up is too long. Security associations (SAs) pause indefinitely during negotiation, and dangling SAs are created at the responder side. This behavior may cause performance degrade for tunnels that have been configured with Dead Peer Detection (DPD).

  Conditions These symptoms are observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(6.8)T2 and that is configured with an Integrated Service Adapter (SA-ISA) that is running hardware encryption.

  Workaround Lower the number of simultaneous IKE sessions.

- CSCdw38678

  Symptoms A Tag Distribution Protocol (TDP) session does not reset.

  Conditions This symptom is observed when you toggle the virtual circuit (VC) merge facility on a label switch controller (LSC).

  Workaround Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on extended Tag (XTag) interfaces.

  Alternate Workaround Toggle the **ip cef** global configuration command.

- CSCdw39338

  Symptoms The low latency queueing (LLQ) “bytes matched” counter that is displayed when the **show policy-map interface** *interface-name* global configuration command is entered is very high.

  Conditions This symptom is observed when Frame Relay encapsulation and interface compression are enabled.

Workaround There is no workaround.

- CSCdw39804

  An interface that was previously configured to perform Frame Relay encapsulation and that has Frame Relay compression enabled may reload if PPP encapsulation is enabled on the interface.

  Workaround: Clear the Frame Relay configuration before configuring PPP encapsulation and passing Real-Time Transport Protocol (RTP) traffic.

- CSCdw40179

  Symptoms A Cisco 6400 series router may reload while PPP sessions are being torn down or when the **show ip access-list** EXEC command or the **show access-lists** EXEC command is entered.

  Conditions This symptom is observed on a Cisco 6400 series platform that is running Cisco IOS Release 12.2(7.4) or a later release and that is functioning as a Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) when you use PPP over Ethernet (PPPoE) with local termination and per-user access control lists (ACLs) from an authentication, authorization, and accounting (AAA) server for the virtual access interfaces.

  Workaround Configure the ACLs on the LAC.

- CSCdw41636

  Symptoms A Cisco router may not forward packets correctly.

  Conditions This symptom is observed on Cisco router that is running a more recent Cisco IOS software release than Cisco IOS Release 12.2(2.3) or Release 12.2(2)T and that is configured to perform User Datagram Protocol (UDP) flooding.

  Workaround Disable Cisco Express Forwarding (CEF) to enable the packets to be forwarded correctly. Disabling CEF may degrade the performance of the router. The level of degradation depends on the features that are related to packet switching and that are enabled on the router.

- CSCdw43127

  Symptoms A Cisco AS5800 that is functioning as a voice gateway may reload because of a software error.

  Conditions This symptom is observed within 5 minutes after the start of a stress test with 60 or more debit card application calls.

  Workaround There is no workaround.

- CSCdw43300

  Symptoms An off-ramp fax Signaling System 7 (SS7) call that is made using a Cisco SC2200 signaling controller may fail.

  Conditions This symptom is observed in Cisco IOS Release 12.2(2)XB2.

  Workaround There is no workaround.

- CSCdw43379

  Symptoms In the short idle period before a router releases a digital signal processor (DSP) after a calling party has hung up, the switch from which the call originated may seize the channel, and instead of the call being released, it is rejected because there is no resource available.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw44548

  Symptoms A router does not block a TCP connection correctly.

Conditions This symptom is observed when the router attempts to deny Secure Shell (SSH) with an access control list (ACL) on vty lines.

The TCP connection should be immediately reset, however, the connection is permitted to be established (that is, a "handshake" occurs), is denied, and then torn down. This behavior may enable a host in the denied ACL to utilize resources on the router (that is, to set up a connection) and possibly prevent legitimate users from being able to access the router via SSH.

Workaround There is no workaround.

- CSCdw45536

  Symptoms On a Cisco AS5300, E1 R2 channels may become blocked after operating normally for a certain period of time and the following message may be displayed:

  ```
  CSM(2/83): Enter csm_enter_disconnecting_state
  VDEV_DEALLOCATE: slot 2 and port 83 is deallocated
  from Trunk(0): (2/20): Tx BWD_CLEAR (ABCD=1101)
  from Trunk(0): (2/20): ignore event
  ```

  Conditions This symptom is observed on a Cisco AS5300 that is connected to E1 R2 channels.

  Workaround There is no workaround.

- CSCdw45708

  Symptoms Ping failures and tracebacks may occur when the **compress stac** interface configuration command is enabled on an 8-port asynchronous and synchronous serial interface.

  Conditions This symptom is observed on a Cisco 2600 series or Cisco 3600 series router that is configured with an 8-port asynchronous and synchronous network module (NM-8A/S) and an Advanced Interface Module (AIM) that is using hardware compression.

  Workaround Use software compression on the serial interfaces.

- CSCdw46926

  Symptoms When an E1 1-port multiflex trunk port adapter is inserted into a voice gateway on a Cisco Catalyst 4000 switch, the E1 card does not come up and the following error message may be displayed:

  ```
  %CONTROLLER-2-FIRMWARE: Controller E1 1/0, firmware is not running
  ```

  Conditions This symptom is observed on a Cisco Catalyst 4000 switch that is running Cisco IOS Release 12.2(5a) or a later release.

  Workaround Use Cisco IOS Release 12.1(5)YF3 instead.

- CSCdw49456

  Symptoms A Voice Response Unit (VRU) is getting digit strings dialed into it when it answers.

  Conditions This symptom is observed on a VRU that is attached to Foreign Exchange Station (FXS) Media Gateway Control Protocol (MGCP) ports.

  Workaround Do not have both Foreign Exchange Office (FXO) and FXS ports on the same gateway if FXO ports are used for dialing out.

- CSCdw50585

  This caveat describes two symptoms, two conditions, and two workarounds:

  Symptoms A The Egress NetFlow feature can be configured on a core Multiprotocol Label Switching (MPLS) interface by using the **mpls netflow egress** command-line interface (CLI) command. However, the Egress NetFlow feature is designed to work only on the outbound Virtual Private Network routing and forwarding (VRF) interfaces of an MPLS network. Enabling it in any other location should be considered a misconfiguration.

Conditions A Conditions do not apply to this situation.

Workaround A Do not configure the Egress NetFlow feature on any MPLS core interface. If the feature is enabled on any MPLS core interface, enter the **no mpls netflow egress** command to disable the feature.

Symptoms B IP packets that are looped back are wrongly accounted for. A new flow in the opposite direction should be created for those IP packets.

Conditions B This symptom is observed on an outgoing MPLS egress flow.

Workaround B There is no workaround.

- CSCdw51651

  Symptoms When you save a router configuration via the Simple Network Management Protocol (SNMP) CISCO-CONFIG-COPY-MIB MIB, the saving process times out.

  Conditions This symptom is observed when a Route Processor Module (RPM) configuration is too large to be stored into NVRAM and you use the CISCO-CONFIG-COPY-MIB MIB to save the configuration. During the execution of the **write memory** command via SNMP, the saving process pauses indefinitely because it incorrectly expects user input.

  Workaround Enter the **rpmnvbypass** command in configuration mode on the RPM to save the configuration on the Processor Switch Module (PXM).

- CSCdw51692

  Symptoms When a Flash disk is used, disk timeout errors such as “ATA_Status time out waiting for 1” may occur.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround Remove and reinsert the disk to restore the disk function.

- CSCdw51821

  Symptoms The cisco-nas-port attribute does not display the correct span number on which a call has been accepted.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw52894

  Symptoms A Cisco 6400 Node Route Processor (NRP) may reload during the execution of the **snmpwalk** command or **snmpget** command on the cdslVcClassTable in the CISCO-DSL-PROVISION-MIB MIB.

  Conditions This symptom is observed on a Cisco 6400 NRP that is running Cisco IOS Release 12.1(5)DC1 and occurs when the NRP is configured with a Virtual Circuit Class (VC Class) that includes parameters that are not supported by the CISCO-DSL-PROVISION-MIB MIB—for example, aal5snap encapsulation or PPP over Ethernet (PPPoE) protocol—and an SNMP retrieval of the entries in the cdslVcClassTable is performed.

  Workaround Configure the **snmp-server view** global configuration command to exclude access of the CISCO-DSL-PROVISION-MIB MIB, in a similar way as in the following example:

  snmp-server view *view-name* **dod included**
  snmp-server view *view-name* **ciscoExperiment.30 excluded**
  snmp-server community *string* **view** *view-name* [**ro**|**rw**]

- CSCdw53195

  Symptoms Memory exhaustion may occur on a Cisco 10000 series router, and the router may reload.

  Conditions This symptom is observed when you copy a configuration file with 32,000 PPP over ATM (PPPoA) sessions with per-session IP quality of service (QoS) policing to the Performance Route Processor (PRP).

  Workaround There is no workaround.

- CSCdw53446

  Symptoms Packets are not marked on a Cisco 7500 router.

  Conditions This symptom is observed when "set xyz" is configured as an action in a modular quality of service (QoS) command-line interface (MQC) service policy that is attached to a distributed Link Fragmentation and Interleaving (dLFI) over Frame Relay link.

  Workaround There is no workaround.

- CSCdw53545

  Symptoms A supported interface is missing when you enter the **busyout monitor** command-line interface (CLI) command.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw54103

  Symptoms The maximum burst size (MBS) value is set to the default value of 32 by variable bit rate non-real-time (VBR-nrt) traffic when the peak cell rate (PCR) is set to be equal to the sustainable cell rate (SCR). The default MBS value of 32 is calculated based on the maximum transmission unit (MTU) of a virtual circuit (VC). (For example, MBS=(MTU/48)+1=(1500/48)+1=32)

  Conditions This symptom is observed on a Cisco 7206VXR router that has an enhanced ATM port adapter (PA-A3) and that is running Cisco IOS Release 12.2.

  Workaround There is no workaround.

- CSCdw54485

  Symptoms A Cisco AS5300 cannot respond to a B12 message that is sent by a switch. This situation affects international nature of address (NOA) calls.

  Conditions This symptom is observed when inbound R2 calls occur.

  Workaround There is no workaround.

- CSCdw54869

  Symptoms A Cisco router may reload with a bus error at an invalid memory location after the **no ip nbar resources** global configuration command is removed.

  Conditions This symptom is observed when the following conditions exist:

  – Network-based application recognition (NBAR) is disabled. Class map, policy map, and service policy statements that are used for NBAR are removed from the configuration.

  – The configuration contains the **ip nbar resources** *max-age initial-links expand-links* global configuration command.

  Workaround Remove the **no ip nbar resources** global configuration command before disabling NBAR.

- CSCdw54940

  Symptoms Outgoing labels become untagged in the Tag Forwarding Information Base (TFIB) when a traffic engineering (TE) tunnel goes down.

  Conditions This symptom is observed on a router that is running Cisco IOS Release 12.0(20.3)ST3, Release 12.0(20.4)ST, Release 12.2 (7.4)T, or Release 12.2(7.6).

  This situation may occur between two label switching routers that have the Label Distribution Protocol (LDP)/Tag Distribution Protocol (TDP) configured on a one-hop tunnel and also on a physical link. When the tunnel goes down, the outgoing label for a prefix that is reachable via a physical link may become untagged.

  Workaround Enter the **clear ip route** *network* EXEC command, in which the *network* argument is the IP address of the TFIB entry that became untagged.

- CSCdw54945

  Symptoms A custom-made Tool Command Language (TCL) 1.0 script that uses a loop to make a series of outbound calls aborts after a few iterations, and the error message "Interpreting too long. Infinite loop?" appears.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw55105

  Symptoms Some channels on a time slot may pause indefinitely in the EM_PENDING state when T1 wink-start signaling is used.

  Conditions This symptom is observed on time slots on a Cisco 3660 router that is running Cisco IOS Release 12.2(7.5) and that has T1 wink-start signaling configured.

  Workaround There is no workaround.

- CSCdw55259

  Symptoms A Cisco 2600 series router may reload because of a bus error. When you enter the **show version** EXEC command, the command output will be very similar to the following:

  ```
  System returned to ROM by bus error at PC 0xXXXXXXXX, address 0xYYYYYYYY
  ```

  0xXXXXXXXX represents the program counter in which the router reloads and 0xYYYYYYYY represents the address where the router reloads.

  The router may also reload at bootup.

  Conditions These symptoms are observed on a Cisco 2600 series router that is configured with a high density voice network module (NM-HDV).

  Workaround There is no workaround. For more information about bus errors, refer to the Cisco document at the following location:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml

- CSCdw55335

  Symptoms If a disconnect message that contains a Progress Indicator (PI) is received on a gateway and the cause code is user-busy, the gateway sends a B6 message on an R2 trunk. The busy tone can then be heard from the terminating switch. Regardless of the PI value, a B3 message should be sent on the R2 trunk, and the PI will then be ignored.

  Conditions This symptom is observed on ISDN or H.323 calls on an R2 trunk when Cisco gateways are used on both sides.

Workaround There is no workaround.

- CSCdw55359

  Symptoms A Cisco 7200 series router may reload.

  Conditions This symptom is observed after the "Enable DSP control message history" option is enabled on the router.

  Workaround To prevent the router from reloading, do not enable the "Enable DSP control message history" option on the router.

- CSCdw55425

  Symptoms Data packets may be dropped during a very short period of time.

  Conditions This symptom is observed when a modulation profile is changed on a Cisco uBR7200 series router.

  Workaround There is no workaround.

- CSCdw55474

  Symptoms The "%VTSP-3-DSP_TIMEOUT: DSP timeout on event 6:" message may be displayed on the console when a call is being set up.

  Conditions This symptom is observed on a Cisco 2600 series, Cisco 3600 series, or Cisco 7200 series router that is configured with a voice digital signal processor (DSP) and that is running Cisco IOS Release 12.2(6a). The DSP resets automatically but the current call is dropped.

  Workaround There is no workaround.

- CSCdw55605

  Symptoms A router may miss an entry in its label forwarding table for a prefix that belongs to a Virtual Private Network (VPN) routing and forwarding (VRF) instance.

  When you enter the **show tag-switching forwarding-table** EXEC command for the missing entry, no label is shown. However, when you enter the **show ip cef detail** EXEC command for the prefix, the correct label is shown.

  Conditions This symptom is observed on a router that is configured as a Multiprotocol Label Switching (MPLS) VPN provider edge (PE) router.

  Workaround There is no workaround. However, if you enter the **clear ip route** EXEC command for the affected prefix, the prefix is reinstalled in the label forwarding table.

- CSCdw57116

  Symptoms The Voice over IP (VoIP) authentication, authorization, and accounting (AAA) process may cause a memory leak during interactive voice response (IVR) calls.

  Conditions This symptom is observed under stress test conditions with debit card application calls or IVR scripts.

  Workaround There is no workaround.

- CSCdw57677

  Symptoms A Cisco 7200VXR series router reloads with the following message:

```
CMD: 'channel-group 3'

%SYS-2-INTSCHED: 'suspend' at level 3
-Process= "Exec", ipl= 3, pid= 2
-Traceback= 606B74AC 606A0288 606A03B8 611ADCC0 611C6CA4 611C6D70 6065D97C 606F6170
606F87D8 60614484 60622C74 60685974 60685960

%Software-forced reload
```

```
Preparing to dump core...
```

Conditions This symptom is observed on a Cisco 7200VXR series router that is running Cisco IOS Release 12.2(6a) when 20 T1 connections are configured, the Transparent Common Channel Signaling (T-CCS) feature is enabled on at least one T1 connection, and you add an IP interface to an EtherChannel group.

Workaround There is no workaround. As a partial workaround, create and bring up the EtherChannel group before you bring up the voice trunks. However, once the voice trunks are up and you add an IP interface that is part of an EtherChannel group, the router will reload.

- CSCdw57901

  Symptoms You cannot configure ISDN service profile identifier 1 (SPID 1) and ISDN SPID 2.

  Conditions This symptom is observed on a Cisco 1700 series, Cisco 2600 series, or Cisco 3600 series router that uses the 2-port ISDN BRI voice interface card, S/T interface, network termination or network terminal equipment (VIC-2BRI-NT/TE) or the 2-port ISDN BRI voice interface card, S/T interface, and terminal equipment (VIC-2BRI-S/T-TE).

  This symptom is also observed on a BRI voice module (BVM) that is installed in a Cisco MC3810.

  Workaround There is no workaround.

- CSCdw58164

  Symptoms A Route Processor Module (RPM) provides an incorrect Cisco Assigned Numbers Authority (CANA) number for the cevChassisRPmmpr chassis value.

  Conditions This symptom is observed when an RPM MIB is accessed by a network management system (NMS).

  Workaround There is no workaround.

- CSCdw58207

  Symptoms A router rejects calls instead of providing plain old telephone service (POTS).

  Conditions This symptom is observed when a dial peer does not explicitly configure an application, for example, when the dial peer does not configure “application default.”

  Workaround Configure “application default” in each dial peer that should be able to use POTS.

  Alternate Workaround Use the hidden **call application fallback default** command-line interface (CLI) command to configure the “default application” that should be used as the fallback application if the application in the dial peer fails.

- CSCdw58272

  Symptoms Modem ISDN Channel Aggregation (MICA) technologies modems may be marked as bad.

  Conditions This symptom is observed after a Cisco AS5800 has been running for more than 10 hours under stress conditions

  Workaround There is no workaround.

- CSCdw59320

  Symptoms The Store and Forward Fax feature fails because of an “RSPREC” error with a disconnect cause of 111.

  Conditions This symptom is observed when a fax call is made from an off-ramp router to an on-ramp router.

  Workaround There is no workaround.

- CSCdw59355

  Symptoms A tunnel may not be established because a router peer may not wait long enough for an offline certification authority (CA) to be discovered.

  Conditions This symptom is observed when a router is configured with the **crl best-effort** command, the certificate revocation list (CRL) is not yet on the router or has expired, and the CA is not online. After the router discovers that the CRL is not available, it continues with the Internet Key Exchange (IKE) negotiations. However the router peer has already timed out.

  Workaround There is no workaround.

- CSCdw59938

  Symptoms A label switch controller (LSC) reloads if an interface on a downstream router is shut down.

  Conditions This symptom is observed when LSCs are configured to use the Tag Distribution Protocol (TDP). The output label switched controlled virtual circuit (LVC) is torn down after the downstream interface is shut down. If the routing protocol has not converged, a new output LVC request is sent to the downstream router using the same interface. When the routing update occurs, the requested output LVC is deleted and the input LVC is released. After the input LVC is released, the LSC will reload if it attempts to delete the output LVC.

  Workaround There is no workaround.

- CSCdw60226

  Symptoms You cannot add virtual connections on a router.

  Conditions This symptom is observed on a Cisco 3662 router that is configured with a single port ATM T3 network module (NM-1A-T3) and that is running Cisco IOS Release 12.2(4)T1.

  Workaround There is no workaround.

- CSCdw61803

  Symptoms When you dial a number, you may hear a tone or beep before you hear the first ringback.

  Conditions This symptom is observed on an R2 digital call.

  Workaround There is no workaround.

- CSCdw63402

  Symptoms When Multilink PPP over ATM (MLPoATM) is configured on a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) network, packets that are not encapsulated by Multilink PPP (MLP) are dropped on the input side.

  Conditions This symptom is observed when the virtual access interface is placed into the VPN routing and forwarding instance (VRF) using RADIUS attributes.

  Workaround Select the VRF by configuring the virtual template using the **ip vrf forwarding** interface configuration command.

- CSCdw63565

  Symptoms A Cisco 7200 series router may reload with a watchdog timer reset.

  Conditions This symptom is observed on a Cisco 7200 series router that is configured with a Network Processing Engine 400 (NPE-400) in a topology in which a call generator is connected over a PRI link to a Cisco 7200 series router that is connected to a second Cisco 7200 series router over an Ethernet link. The second Cisco 7200 series router is connected to another call generator.

  Workaround There is no workaround.

- CSCdw63657

  Symptoms Spurious memory accesses are observed at the dsx3_controller_t1_framing process. Spurious memory accesses may also occur if a router is rebooted while framing is set to extended super frame (ESF).

  Conditions This symptom is observed when ESF framing is configured on a Channelized T3 Interface Processor (CT3IP) controller.

  Workaround There is no workaround.

- CSCdw64077

  Symptoms A Cisco 7500 series router may not pass traffic through a Multilink PPP (MLP) group interface over a nonchannelized interface.

  Conditions This symptom is observed when distributed Cisco Express Forwarding (dCEF) is enabled.

  Workaround Disable dCEF.

  Alternate Workaround Configure a virtual template to bundle MLP links.

- CSCdw64914

  Symptoms The following message may appear at the end of a call:

  ```
  vnm_dsprm_tdm_info_null - bad parametera (0x81836840, 0x818 1F09C, 0, 1, 0x0)
  ```

  Call functionality does not seem to be impacted.

  Conditions This symptom is observed on a Cisco VG200.

  Workaround There is no workaround.

- CSCdw67561

  Symptoms Border Gateway Patrol (BGP) silently ignores a password that has fewer than four characters but does not authenticate the BGP session. When you enter the **show configuration** EXEC command, the ignored password is displayed.

  Conditions The conditions under which these symptoms occur are not known at this time.

  Workaround Use a password that has more than four characters.

- CSCdw67688

  Symptoms A UPC324 universal port card may reload, which may trigger the router shelf to reload.

  Conditions This symptom is observed on a Cisco AS5800.

  Workaround There is no workaround.

- CSCdw68449

  Symptoms The following error message may appear on a router shelf:

  ```
  Zulu: %SYS-3-NOELEMENT: data_enqueue:Ran out of buffer elements for enqueue
  -Process= "TTY Background", ipl= 4, pid= 31
  -Traceback= 60510EE0 604B75EC 604B7A40 604B7D94 604D2F38 6054D65C 6054D648
  ```

  Conditions This symptom is observed during the reboot process of a Cisco AS5800 that is running Cisco IOS Release 12.2(7).

  Workaround There is no workaround.

- CSCdw68712

  Symptoms A caller does not hear a ringback when a call is made when the Session Initiation Protocol (SIP) is enabled.

  Conditions This symptom is observed on an originating gateway (OGW) that is running a special Cisco IOS image that does not support ISDN progress messages when the terminating gateway (TGW) is running Cisco IOS Release 12.2(2)XA3 or Cisco IOS Release 12.2(2)XB4 and has the **voice call send-alert** global configuration command enabled.

  Workaround Disable the **voice call send-alert** global configuration command on the TGW.

- CSCdw69187

  Symptoms Cisco IOS software may not recognize the online insertion and removal (OIR) of a port adapter, and OIR events may not be captured.

  Conditions This symptom is observed on a Cisco 7200 or Cisco 7400 router that has a Network Service Engine-1 (NSE-1) while the Level 3 (L3) Cache Bypass feature is enabled. The Cisco 7400 has to be reloaded before a new port adapter is recognized.

  Workaround Avoid using the L3 Cache Bypass feature on a Cisco 7200 or Cisco 7400 that has an NSE-1 if the installation of a port adapter using an OIR procedure is anticipated.

- CSCdw69681

  Symptoms One-way audio may occur and a caller who is using an IP telephone may not be able to hear the caller at the Public Switched Telephone Network (PSTN) side. No Real-Time Protocol (RTP) packets seem to be sent to the caller using the IP telephone.

  The **debug cch323 rtp** command and the **show call active voice brief** EXEC command indicate that RTP packets are sent and received. However, the call statistics on the IP phone indicate that no RTP packets are received.

  Conditions These symptoms are observed in Cisco IOS Release 12.2(6B) when you enable the **h323-gateway voip bind srcaddr** interface configuration command on an interface.

  Workaround To restore two-way audio, disable the **h323-gateway voip bind srcaddr** interface configuration command.

  Alternate Workaround Use the **h323-gateway voip bind srcaddr** interface configuration command to designate the IP address of a loopback interface instead of a physical interface.

- CSCdw69768

  Symptoms A headend edge label switch router (ELSR) may generate unsynchronized tag bindings and display the following error message:

  ```
  %SCHED-3-THRASHING: Process thrashing on watched managed timer (0x414A4920).
  -Process= "TC-ATM Proc", ipl= 4, pid= 88 -Traceback= 40398AC0 40398EC0 4099DF14
  ```

  Conditions These symptoms are observed in a cell-based Multiprotocol Label Switching (MPLS) setup. These symptoms are observed on the headend ELSR after the tailend of an ELSR tag distribution protocol (TDP) or label distribution protocol (LDP) session is toggled. These symptoms occur because the headend ELSR does not clean up all tag bindings completely after the TDP or LDP session goes down. The headend ELSR keeps the state of some of the stale tag bindings as active.

  Workaround When this symptom occurs, the user can toggle the headend TDP or LDP session by issuing the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command either on the extended tag ATM (XTagATM) interface on the label switch controller (LSC) or on the MPLS subinterface on the headend ELSR.

- CSCdw71400

  Symptoms An invalid cache adjacency exists on a line card but not on the Route Processor (RP)

  Conditions The conditions under which these symptoms occur are not known at this time.

  Workaround Enter the **clear cef linecard** *slot-number* **adjacency** EXEC command on the line card.

- CSCdw71419

  Symptoms The CiscoFlashFileTable loops during a Simple Network Management Protocol (SNMP) walk.

  Conditions This symptom is observed on a Cisco 6400 Node Switch Processor (NSP) when you create a file in a Personal Computer Memory Card International Association (PCMCIA) device without rebooting the NSP.

  Workaround There is no workaround.

- CSCdw71436

  Symptoms A Cisco router may reload because of a segmentation violation (SegV) when fax calls are present.

  Conditions This symptom is observed under rare circumstances.

  Workaround There is no workaround.

- CSCdw72513

  Symptoms A permanent virtual connection (PVC) bundle does not go down when the implicit bumping method is enabled and when a member of the PVC bundle cannot be bumped implicitly.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw73961

  Symptoms Low throughput may occur on a Cisco 7500 series router that is configured with a PA-MC-T1 or PA-MC-E1 port adapter that is part of a multilink connection that has weighted fair queuing (WFQ) configured.

  Conditions This symptom is observed after you enter the **shutdown** controller configuration command followed by the **no shutdown** controller configuration command on the controller of the port adapter or after you reboot the router.

  Workaround Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the multilink interface.

  Alternate Workaround Use distributed switching.

- CSCdw74143

  Symptoms A Cisco 7500 series Route Switch Processor (RSP) reloads when a policy map is associated to a Frame Relay map class.

  Conditions This symptom is observed on a router that has 380 interfaces configured and each interface has distributed Frame Relay fragmentation (dFRF.12) configured.

  Workaround There is no workaround.

- CSCdw76315

  Symptoms Some digital signal processors (DSPs) may periodically display the following message on the console and pause indefinitely:

  ```
  %VTSP-3-DSP_TIMEOUT: DSP timeout on event 6: DSP ID=0x1: DSP error stats, chnl info(4,
  7, 0)
  ```

Conditions This symptom is observed on a digital Foreign Exchange Office Loop Start (FXOLS) to analog Foreign Exchange Station Loop Start (FXSLS) connection trunk network that has the FXOLS voice ports configured on a Cisco 7200 router that has a 2-port T1, E1 enhanced digital voice plus port adapter (PA-VXB-2TE1+) or a 2-port T1, E1, high capacity, enhanced digital voice port plus adapter (PA-VXC-2TE1+). The analog FXSLS voice ports are provided by a voice network module that has voice interface card (VIC) slots (NM-1V or NM-2V) on a Cisco 2600 or 3600 router.

This symptom is triggered when compressed Real-Time Transport Protocol (cRTP) is configured on a WAN link that exists between the two voice gateways, when a connection trunk is configured for voice services, and when fast switching is enabled on the interface that has cRTP configured.

Workaround Stop using cRTP or disable fast-switching on the WAN interface by entering the **no ip route-cache** interface configuration command. This symptom does not occur if process-switched cRTP is used.

The fix for this caveat is applied via the **ip rtp coalesce** global configuration command in Cisco IOS images. Fast switching can remain enabled on the cRTP interfaces. The new **ip rtp coalesce** global configuration command will not increase the CPU load appreciably above normal fast switching cRTP levels.

- CSCdw76822

  Symptoms IP connectivity may be disrupted after distributed Cisco Express Forwarding (dCEF) is configured on a router.

  Conditions This symptom is observed on a Cisco 7500 series router that is functioning as a provider edge (PE) router and that is running tag switching or Multiprotocol Label Switching (MPLS). This symptom occurs if the router is running both cell-based and frame-based tag switching simultaneously.

  Workaround There is no workaround.

- CSCdw77623

  Symptoms The authentication, authorization, and accounting (AAA) command authorization may fail.

  Conditions This symptom is observed when the user profile on the AAA server contains the remote client address or the teletype (tty) name for the EXEC session.

  Workaround Remove references to the remote client address and tty name in the user profile on the AAA server.

- CSCdw80181

  Symptoms The system returns to the ROM monitor (ROMmon) prompt.

  Conditions This symptom is observed after a watchdog timer expires.

  Workaround There is no workaround.

- CSCdw80326

  Symptoms Entering the **no access-list 101** command in configuration mode causes a router to reload because of a bus error.

  Conditions This symptom is observed when comments along with dynamic access control entries (ACEs) are used in the access control list (ACL) that is being removed.

  Workaround Do not use comments for dynamic ACEs in an ACL. Comments for nondynamic ACEs do not cause the symptoms to occur.

- CSCdw80521

  Symptoms If an access server is configured for resource pooling with customer profile templates, a short, abnormal call may cause the next call on the same modem or interface to bind to multiple profiles, resulting in the configuration for this call to be different than intended.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround Ensure that each customer profile template explicitly specifies every configuration item that may differ from other customer profile templates so that the configuration items on the intended template override any configuration items on other templates that may unexpectedly be bound. The workaround does not work when multiple short, abnormal calls that are accepted on the same port consecutively.

- CSCdw80542

  Symptoms The portware download process may take 85 to 90 percent CPU utilization, which leads an overall CPU utilization of 99 percent.

  Conditions This symptom is observed after a Cisco AS5800 that is running Cisco IOS Release 12.2(7) has reloaded.

  Workaround Reload the router again.

- CSCdw80730

  Symptoms Dynamic crypto map sets with several entries do not work. Any traffic that does not match the first dynamic crypto map within the set is discarded. If you enable the **debug crypto engine** command, the following message is logged:

  ```
  'CRYPTO: Packet dropped because of an incomplete cryptomap'
  ```

  Conditions This symptom is observed in Cisco IOS Release 12.2.

  Workaround Place each dynamic crypto map template within its own dynamic crypto map set.

- CSCdw81809

  Symptoms Dial calls may go through, but a mismatch in answering signals may occur for Voice over IP (VoIP) calls and the VoIP calls may not work with some telecommunication switches.

  Conditions This symptom is observed when an E1 R2 trunk is configured on a Cisco AS5300. Because answering signals are not configurable for outgoing calls, this situation has to be addressed in the country table and the Finite State Machine (FSM).

  Workaround There is no workaround.

- CSCdw82351

  Symptoms A Cisco gateway that is running a voice application may reload under a heavy load.

  Conditions This symptom is observed on a Cisco gateway that is running Cisco IOS Release 12.2(8)T, Release 12.2(2)XU, or Release 12.2(2)XB3 when Signaling System 7 (SS7) ISDN User Part (ISUP) transparency is used or when a large amount of information about supplementary services is passed.

  Workaround There is no workaround.

- CSCdw82553

  Symptoms A network access server (NAS) may continuously send an out of service (OOS) message for a Non-Facility Associated Signaling (NFAS) group.

  Conditions This symptom is observed on a Cisco AS5800 in a configuration with multiple NFAS groups.

  Workaround There is no workaround.

- CSCdw85034

  Symptoms A memory leak may occur when a Simple Network Management Protocol (SNMP) get or getnext request is performed.

  Conditions This symptom is observed when an SNMP get or getnext request is performed on the cdslLocalIpAddrPoolTable and cdslLocalIpAddrRangeTable tables of the CISCO-DSL-PROVISION-MIB MIB.

  Workaround There is no workaround.

- CSCdw85558

  Symptoms On a Cisco 7200 series router that is configured with a 2-port T1/E1 moderate capacity port adapter (PA-VXB) or a 2-port T1/E1 high-capacity port adapter (PA-VXC), you do not have the option to configure the **channel-group** controller configuration command, which makes it impossible to configure the **mode ccs frame-forwarding** controller configuration command.

  Conditions This symptom is observed in Cisco IOS Release 12.1(3a)T1, Release 12.1(5)T9, Release 12.2(6a), Release 12.2(7a), and Release 12.2.(7.6).

  Workaround Run Cisco IOS Release 12.2 T so that you have the command-line interface (CLI) to configure the **mode ccs frame-forwarding** controller configuration command.

  Alternate Workaround Enable the **codec clear-channel** command.

- CSCdw86466

  Symptoms The input queue fills and the Systems Network Architecture Switching Services (SNASw) upstream link fails.

  Conditions This symptom occurs if SNASw receives a protocol violation generating sense 8007 on an incoming bind frame from the virtual telecommunications access method (VTAM). This situation causes subsequent frames to be kept on the input hold queue. This behavior causes failures with sense 0805 on the VTAM, causing sessions to be stuck in the “pending session start” (PSEST) state. When this condition occurs, the input queue eventually fills and the SNASw upstream link fails.

  Workaround Identify and terminate the affected Real-Time Transport Protocol (RTP) pipe from the VTAM.

- CSCdw86740

  Symptoms The service policy overruns the interprocess communications (IPC) mechanism on a Cisco 7500 series router.

  Conditions This symptom is observed when a service policy is applied to a large number of interfaces simultaneously.

  Workaround Break up the service policy and apply the service policy individually to a smaller group of interfaces.

- CSCdw86905

  Symptoms The **huntstop** dial-peer configuration command does not function. When a call fails on the first dial peer, the call attempts to go out on the second dial peer, even when the **huntstop** dial-peer configuration command configured on the first dial peer.

  Conditions This symptom is observed when a call that is made on the first dial peer fails in the alerting state.

  Workaround There is no workaround.

- CSCdw89199

  Symptoms When a terminating gateway (TGW) has a dial-peer definition that matches a called number but a PBX returns an "unallocated/unassigned number" message, the message is passed end-to-end without problems. However, when the TGW does not have a dial-peer definition that matches the called number, the originating gateway (OGW) sends a "call rejected" cause code, which is incorrect behavior.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw89528

  Symptoms A service policy that is applied to an Ethernet subinterface does not work.

  Conditions This symptom occurs after a policy map is applied to an outbound Ethernet subinterface. The service policy works if the policy is applied to the main Ethernet interface, but the service policy does not work if it is attached to a subinterface. When this symptom occurs, the class of service (COS) bit above 0 on Layer 2 of the Ethernet Frame is not set.

  Workaround Apply the service policy to the main Ethernet interface.

- CSCdw90119

  Symptoms Ethernet bridge-encapsulated ATM packets (mandated by RFC 1483) may be sent out with nonzero pad bytes (2 bytes) in the header.

  Conditions This symptom is observed when ATM routed bridge encapsulation (RBE) is used with Cisco Express Forwarding (CEF) switching and Ethernet bridge-encapsulated ATM packets are sent. Although the RFC does not mandate that the two pad bytes have to be zeroed, some bridges may require the padding bytes to be zeroed.

  Workaround Enter the **clear adjacency** EXEC command to clear the CEF adjacency table.

- CSCdw90464

  Symptoms A Cisco router may not accept the **ds0-group** controller configuration command for a T1 or E1 controller.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw90486

  Symptoms Differentiated services code point (DSCP) or type of service (ToS) based class-based weighted fair queueing (CBWFQ) traffic classification may not work with hardware accelerator cards.

  Conditions This symptom is observed on a Cisco 2600 router that is using an advanced integration module (AIM) Virtual Private Network (VPN) card and that has CBWFQ, IP Security (IPSec), and generic routing encapsulation (GRE) enabled. The Cisco 2600 is running Cisco IOS Release 12.2(7a). The same configuration works normally if software encryption is used.

  Workaround Use Cisco IOS Release 12.2(2)T or a later release.

  Alternate Workaround Use process switching.

- CSCdw91554

  Symptoms A router may reload when the **show snasw port** command is enabled.

  Conditions This symptom is observed on a Systems Network Architecture Switching Services (SNASw) router that is running Cisco IOS Release 12.2(8.4) and that has one port configured for High Performance Routing (HPR)/IP.

Workaround Do not use the **show snasw port** command. You can monitor ports via Simple Network Management Protocol (SNMP) or via CiscoWorks Blue Maps.

- CSCdw92846

  Symptoms Dangling digital signal processors (DSPs) may occur on a universal access server.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that is configured as both an outgoing gateway (OGW) and a terminating gateway (TGW) and that is running Cisco IOS Release 12.2(6). The number of dangling DSPs remains in the dangling state and continues to increase as time passes. This symptom occurs only if there is no matching dial peer for the calls that are coming in from the ISDN side.

  Workaround Ensure that there are matching dial peers for calls that originate from the ISDN side.

- CSCdw94532

  Symptoms A router may experience digital signal processor (DSP) timeouts and show an error message similar to the following error message:

  ```
  CET: dsp 6 is not responding
  CET: dsp 14 is not responding
  ```

  Conditions This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(6a) or Release 12.2(9).

  Workaround There is no workaround.

- CSCdx02036

  Symptoms If the prefix of a provider edge (PE) router is learned over a Packet over SONET (POS) interface, the prefix is untagged.

  Conditions This symptom is observed in a Carrier Supporting Carrier (CsC) topology in which two Cisco PE routers are connected to a POS interface. The prefix of the PE router is untagged after the topology is configured if the prefix is learned over a POS interface. When this symptom occurs, traffic forwarding through the CsC core is stopped.

  Workaround Manually clear the prefix from the routing table and establish a tag for the prefix.

- CSCdx03069

  Symptoms A memory leak may occur on an H.323 voice gateway.

  Conditions This symptom is observed when the connected gatekeeper sends an admission confirm (ACF) message with the destination Call Signal Address (dCSA) field set to 0.0.0.0 and when the alternate endpoint field is present in the message.

  Workaround There is no workaround.

- CSCdx04605

  Symptoms A memory leak may occur on a Cisco gateway, and eventually the gateway becomes unresponsive and reboots automatically.

  Conditions This symptom is observed when the Cisco gateway receives an H.225 setup message that contains one or more clearTokens and any information in the nonStandardData field.

  Workaround There is no workaround.

- CSCdx06503

  Symptoms The **ip director host verify-url** global configuration command cannot determine if a server is properly available. The command may not even reach the service port, but behaves as if the server is up.

  Conditions This symptom is observed on a Cisco DistributedDirector.

Workaround There is no workaround.

- CSCdx08669

  Symptoms A Cisco 7500 series router experiences spurious memory accesses and reloads with a bus error.

  Conditions This symptom is observed on a Cisco 7500 series router that is running the rsp-pv-mz image of Cisco IOS Release 12.0(16)ST and that has Multiprotocol Label Switching (MPLS) enabled. This situation is related to the use of the **aggregate-address** Border Gateway Protocol (BGP) command.

  Workaround There is no workaround.

- CSCdx13597

  Symptoms A router reloads when you enter the **show tag-switching tdp neighbors** EXEC command.

  Conditions The conditions under which these symptoms occur are not known at this time.

  Workaround There is no workaround.

- CSCdx14383

  Symptoms A memory leak may occur when an E1 controller uses E1-R2 signaling.

  Conditions This symptom is observed on an E1 controller that is installed on a Cisco AS5300 universal access server that using E1-R2 signaling and that is running Cisco IOS Release 12.2(7). This symptom can be verified by examining the command output of the **show chunk | beg vtsp** EXEC command:

  ```
  1320     8  2276     537        0     537        0 VTSP EVENT pool 0x618CC5C8
  1320     8 713180     537        0     537        0 (data) 0x622BCA58
  32     0   852      20        0      20        4 Call Management 0x6182D0D0
  ```

  The value 0 (bold in the output above) indicates the number of voice telephony security parameter (VTSP) EVENT chunks that are in use. This value should be 0 if no calls are present (as in the case of the command output that is shown above). This value changes according to the number of active calls. A continuous increase of this value indicates that VTSP EVENT memory is not being released, eventually resulting in chunk memory allocation (MALLOC) failures.

  Workaround There is no workaround.

- CSCdx16376

  Symptoms A router may reload because of a bus error and display the following message when the **show version** EXEC command is issued:

  ```
  System returned to ROM by bus error at PC 0xXXXXXXXX, address 0xXXXXXXX
  ```

  Conditions This symptom is observed on a Cisco AS5800 universal access server that is running T1 channel-associated signaling (CAS) or the E1 R2 protocol under a heavy load.

  Workaround There is no workaround.

- CSCdx16714

  Symptoms A Route Processor (RP) may experience a bus error or pause indefinitely when a crash test is performed.

  Conditions This symptom occurs after the **test crash** command is issued on an active RP.

  Workaround Reload or power-cycle the router.

- CSCdx24321

  Symptoms An asynchronous modem call may not come up.

Conditions This symptom is observed on a Cisco AS5800 universal access server that is running Cisco IOS Release 12.2(9.4).

Workaround Use Cisco IOS Release 12.2(9.3).

- CSCdx34351

  Symptoms The Open Settlements Protocol (OSP) does not try all destinations that are returned from the OSP server. When an OSP server returns multiple destinations in the AuthorizationResponse message, a gateway does not attempt to set up the call using one of the destinations until a call is successful or until the list is exhausted.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that is used as an outgoing gateway and that is running Cisco IOS Release 12.2(9.2). If a terminating gateway fails to validate the token from a call that is made from the outgoing gateway, the outgoing gateway stops and does not attempt to set up the call to the second destination or report source usage indication.

  Workaround There is no workaround.

- CSCin00398

  Symptoms A Cisco router may reload at the voip-rtcp-new process.

  Conditions This symptom is observed in various test scenarios and occurs only when Session Initiation Protocol (SIP) is used as the call control protocol. The symptom does not occur when H.323 is used. The router reloads during functionality testing but not stress or load testing and typically after making seven to ten successive calls.

  Workaround There is no workaround.

- CSCin00545

  Symptoms Packets are switched by a Route Switch Processor (RSP) instead of a Versatile Interface Processor (VIP) when distributed Cisco Express Forwarding (dCEF) is enabled.

  To determine if this condition is occurring, enter the **show ip cef summary** EXEC command and the **show cef interface** EXEC command on the RSP and the VIP. The router is switching using Cisco Express Forwarding (CEF) via the RSP instead of the VIP if you receive the following output when you enter each of the commands on the RSP and the VIP:

  ```
  RSP# show ip cef summary
  IP Distributed CEF with switching

  VIP# show ip cef summary
  IP Distributed CEF without switching

  RSP# show cef interface
  POS4/0/0 is up (if_number 22) IP Feature CEF switching turbo vector

  VIP# show cef interface
  POS4/0/0 is up (if_number 22) IP VIP to RSP switching turbo vector
  ```

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCin01252

  Symptoms A router may experience a line protocol flap or go down in high traffic conditions.

  Conditions This symptom is observed on a Cisco 7200 router that has a port adapter (PA-T3, PA-E3, or PA-H), a Network Processing Engine (NPE-400), or a Network Service Engine-1 (NSE-1).

  Workaround Use dual interface versions of the port adapters mentioned above.

- CSCin01394

  Symptoms A Cisco 7500 series router displays the following error messages:

```
%SRP-4-ALARM: SRP0/0/0 Side B Keepalive Failure (MAC) %SRP-4-WRAP_STATE_CHANGE:
SRP0/0/0 wrapped on side A (side B Self Detect Signal Fail) %SRP-4-ALARM: SRP0/0/0
Side B Keepalive OK
```

Conditions This symptom is observed on a Cisco 7500 series router that is running Cisco IOS Release 12.0(21)S and through which no traffic is flowing.

Workaround There is no workaround.

- CSCin02629

  Symptoms A Cisco Voice over IP (VoIP) gateway may fail to provide a ringback tone to a calling party when the called party is alerted.

  Conditions This symptom is observed when the VoIP gateway is configured for interactive voice response (IVR).

  Workaround Replace IVR with the default application.

- CSCin02715

  Symptoms Traffic is not sent out of a spatial reuse protocol (SRP) interface.

  Conditions This symptom is observed on a Cisco 7500 series router when distributed Cisco Express Forwarding (dCEF) is enabled on an interface that is used to route both SRP and IP traffic.

  Workaround Change from first-in first-out (FIFO) to priority queueing (PQ).

- CSCin03199

  Symptoms A Cisco gatekeeper may reload when it forwards a location request (LRQ) to a remote cluster.

  Conditions This symptom is observed on a Cisco gatekeeper that is running Cisco IOS Release 12.2(8)T and that is functioning as a directory gatekeeper (DGK), and occurs only if the DGK has a remote cluster configuration.

  Workaround There is no workaround.

- CSCin03257

  Symptoms A back-to-back ping for multilink fails.

  Conditions This symptom is observed when you have the **multilink min-links** *links* command configured on the multilink interface.

  Workaround Enter the **shutdown** interface configuration command on the multilink interface, wait for the multilink and the member links to go down, and enter the **no shutdown** interface configuration command on the multilink interface. After the multilink comes up, the back-to-back ping for multilink will work.

- CSCin04187

  Symptoms A Dynamic Host Configuration Protocol (DHCP) client may not send the correct host name in the DHCP host name feature (option 12) even after the correct host name is configured by entering the **ip address dhcp** *host-name* global configuration command. An incorrect host name is displayed when the **show running-config** EXEC command is entered.

  Conditions This symptom is observed in images of Cisco IOS Release 12.2 and Release 12.2 T that contain the fix for caveat CSCdu62830.

  Workaround There is no workaround.

- CSCin04813

  Symptoms Voice digital signal processors (DSPs) are not detected by a router. The output of the **show interface dspfarm dsp** privileged EXEC command states “no dsps present,” but when you reload the router, all the DSPs come up.

Conditions This symptom is observed on a Cisco 7500 series router that is configured with a 2-port T1/E1 high-capacity port adapter (PA-VXC-2TE1) that is configured for T1 or E1.

Workaround Reload the router after configuring the PA-VXC-2TE1 for T1 or E1.

- CSCin04953

  Symptoms If a channel group number is greater than 23, a router reloads.

  Conditions This symptom is observed on a 2-port T1/E1 high-capacity, enhanced port adapter (PA-VXC-2TE1+) that is configured as a T1 controller.

  Workaround Do not configure a channel group number that is greater than 23 when the PA-VXC-2TE1+ is configured as a T1 controller.

- CSCin08849

  Symptoms If the first dial peer routes and authorizes a call using the Open Settlement Protocol (OSP), subsequent attempts to set up the call with the rest of the dial peers on the list do not work.

  Conditions This symptom is observed when a dial peer rotary is used with OSP.

  Workaround There is no workaround.

- CSCuk27655

  Symptoms Generic routing encapsulation (GRE) is not compliant with RFC 2784 and RFC 2890.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCuk29628

  Symptoms You may not be able to use Cisco Express Forwarding (CEF) commands to enable CEF, and packets may be process-switched.

  Conditions This symptom is observed on a Cisco 7100 series router.

  Workaround There is no workaround.

- CSCuk30474

  Symptoms A line card may be stuck in an off-for-download state. This condition is indicated by the output of the **show cef linecard** EXEC command.

  Conditions This symptom is observed on a Cisco 7500 series router or a Cisco 12000 series Internet router and is caused by an interprocess communication (IPC) error with another line card during the Forwarding Information Base (FIB) table download process.

  Workaround There is no workaround.

Protocol Translation

- CSCdw58040

  Symptoms A Point-of-Sale (PoS) terminal router generates the traceback messages and does not disconnect a call after the timeout expires. The following traceback messages are generated:

```
-Process= "TTY Background", ipl= 0, pid= 18
-Traceback= 80318450 803160F4 8028D5E0 8028CD1C 8028E4E4 8028E7E8 8028EC74 8032DF38
%SYS-3-TIMERNEG: Cannot start timer (0x80DF2F28) with negative offset (-100665).
-Process= "TTY Background", ipl= 0, pid= 18
```

  Conditions These symptoms are observed during an X.25 call over an X.28 packet assembler/disassembler (PAD).

  Workaround In order not to have traceback messages being generated, enter the **no exec-timeout** line configuration command on the vty line on which the X.25 call is made.

  In order not to have the connection time out, enter the **session-timeout** *minutes* line configuration command on the line from where the connection is initiated. Note that changing the **session-timeout** *minutes* line configuration command affects all the connections that are made from this line.

TCP/IP Host-Mode Services

- CSCds29458

  Symptoms A Cisco 7500 series router may run low on stack memory, produce error messages similar to the following messages, and reload because of a software condition:

```
UTC-08d: %TCP-2-INVALIDTCB: Invalid TCB pointer: 0x61C176BC
-Process= "Exec", ipl= 0, pid= 27
-Traceback= 6032FC8C 6032C5F8 60334080 601B0B3C 6033900C 603344D8 603350F8 60331544
60863C88 60870B90 6086427C 6033409C 601B0B3C 6033900C 603344D8 603350F8
UTC-08d: %SYS-6-STACKLOW: Stack for process Exec running low, 0/12000
```

  Conditions This symptom is observed on a Cisco 7500 series router that is configured with one or more Channel Interface Processors (CIPs) and that is using the TN3270 application.

  Incorrect behavior during the closing of TCP connections (which may be related to the TN3270 application) may cause the TCP output code to get stuck in a loop, which eventually uses up all of the memory of the stack and causes the router to reload.

  Workaround There is no workaround.

- CSCdv28984

  Symptoms An access server may generate a Simple Network Management Protocol (SNMP) trap for each single TCPClear call.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw58350

  Symptoms The Karn's Round-Trip Time (KRTT) may not be bound to the round-trip timeout (RTTO).

Conditions This symptom is observed on a Cisco router that is running a Cisco IOS release that contains the fix for caveat CSCdu18397. When there are retransmissions that occur between the TCP endpoints, the KRTT value can become excessively large and the TCP connection drops. This situation frequently affects data-link switching (DLSw). The DLSw peers sporadically drop.

Workaround There is no workaround.

Wide-Area Networking

- CSCdr25383

  The load on a bri0:0 interface (D channel) never increases and always remains at 1/255. There is no workaround.

- CSCdu09850

  The command output of the **show frame-relay pvc** [**interface** *interface* [*dlci*]] privileged EXEC command may display only information about the permanent virtual connection (PVC) status between two switches. The command output does not display information related to the PVC that is received from the Local Management Interface (LMI) on the Network-to-Network Interface (NNI) link. This condition was observed on a Cisco Catalyst 8540 switch that was running Cisco IOS Release 12.0(13). There is no workaround.

- CSCdu09927

  A Cisco 3600 router that is running Cisco IOS Release 12.1(5)T5 may experience a memory leak in the ISDN process. There is no workaround.

- CSCdu60305

  Symptoms A Gigabit Ethernet Interface Processor (GEIP) reloads because of memory corruption.

  Conditions This symptom is observed when Inter-Switch Link (ISL) encapsulation is enabled on an interconnected Gigabit Ethernet interface and traffic is flowing between two routers that are connected or an information exchange of keepalives or of Cisco Discovery Protocol (CDP) occurs

  Workaround There is no workaround.

- CSCdv22568

  Symptoms A memory leak may occur on a router.

  Conditions This symptom is observed on a Cisco router that is configured for X.25 over the Link Access Procedure, Balanced (LAPB) links in a high-error environment.

  Workaround Correct the cause of the high-error rate on the LAPB links.

- CSCdv22680

  Symptoms A Cisco AS5300 may reload repeatedly with a corrupted counter.

  Conditions This symptom is observed on a Cisco AS5300 that is running Cisco IOS Release 12.1(6.01) or Release 12.2(8) and that has ISDN large-scale dial-out (LSDO) configured in a point of presence (POP) with Multilink PPP (MLP).

  Workaround There is no workaround.

  There is no workaround.

- CSCdv29225

  On a Cisco AS5300 universal access server that is running Cisco IOS Release 12.2(2)XA1 in a Signaling System 7 (SS7) Interconnect for Voice Gateway solution, if a call is made ingress to the solution from a Public Switched Telephone Network (PSTN) and if a requested continuity test

(COT) fails, the Cisco SC2200 signaling controller will send a group service message to the Cisco AS5300 and put the associated channel on the access server into the maintenance state. However, the Cisco AS5300 puts the associated channel into the idle state a few seconds later. This behavior creates a mismatch in the channel state between the signaling controller and the Cisco AS 5300. There is no workaround.

- CSCdv34579

  Symptoms A Versatile Interface Processor (VIP), Gigabit Ethernet Interface Processor (GEIP), Gigabit Ethernet Interface Processor plus (GEIP+), or Packet OC-3 Interface Processor (POSIP) that is installed in a router may reload. The VIP may display the following error message when it reloads:

  ```
  %DMA-1-DRQ_STALLED: DRQ stalled. Dumping DRQ.
  ```

  Conditions This symptom is observed on a Cisco 7500 router under heavy traffic conditions.

  Workaround There is no workaround.

- CSCdv50106

  Symptoms PPP callback with bilateral authentication may fail intermittently because the authentication does not complete before the caller hangs up to receive the callback.

  Conditions The occurrence of this condition depends on the debugs that are configured, the switch speed, and the speed of the router.

  Workaround Configure authentication on only the router that is called.

- CSCdv57640

  This caveat describes two symptoms, two conditions, and two workarounds:

  Symptoms A Only about 50 percent of data packets are able to make it across a tunnel.

  Conditions A This symptom is observed when a virtual-template interface is configured for IP virtual routing and forwarding (VRF) in a Layer 2 Tunnel Protocol (L2TP) dial-in setup.

  Workaround A Disable the **ip route-cache cef** and the **ip route-cache** interface configuration commands on the virtual template interface to allow all packets to go through the process-switching.

  Symptoms B Counters on the virtual access interfaces that are used for L2TP sessions on an L2TP access concentrator (LAC) or an L2TP network server (LNS) show incorrect values.

  Conditions B This symptom is observed when IP Cisco Express Forwarding (CEF) is enabled on high-end routers.

  Workaround B There is no workaround.

- CSCdv79935

  Symptoms When multilink with caller ID callback is configured, only the first call is called back. Remaining calls are not called back.

  Conditions This symptom is observed only in a multilink configuration.

  Workaround Use PPP callback to call back multiple links.

- CSCdv88097

  A Cisco 7200 router that is running Cisco IOS Release 12.2(5) and that is acting as a Layer 2 Tunneling Protocol Network Server (LNS) may reload with an error interrupt while it is receiving malformed packets that have payload data (such as User Datagram Protocol [UDP]) that is invalid. There is no workaround.

- CSCdv88102

  With some RSP-PV software images for a Cisco 7500 router that has a Versatile Interface Processor (VIP), certain **x25** commands such as the **show x25** EXEC command cannot be used. This condition applies only to images that belong to the service provider feature set. This condition does not affect the overall functionality for the X.25 signaling type or X.25 configuration commands.

  Workaround: Use another feature set.

- CSCdw01642

  Symptoms A Cisco AS5800 may reload because of a bus error at PC 0x603D2EC4, address 0xC.

  Conditions This symptom is observed on a Cisco AS5800 that is running Cisco IOS Release 12.2.

  Workaround There is no workaround.

  Note After this fix, counters on the virtual access interfaces that are used for Layer 2 Tunnel Protocol (L2TP) sessions on an L2TP access concentrator (LAC) or an L2TP network server (LNS) show incorrect values when IP Cisco Express Forwarding (CEF) is enabled on high-end routers. The fix for caveat CSCdv57640 resolves this condition.

- CSCdw04802

  The virtual-access counters and the RADIUS accounting data exceed the real value. This condition was observed on a Cisco 7200 PA-A3 port adapter and a Cisco 6400 NRP2-SV when a Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) used an ATM permanent virtual connection (PVC) as an ingress interface for L2TP tunnels.

  Workaround: Use xEthernet as the ingress interface.

- CSCdw08887

  Symptoms When the ring-again feature is used between PBXs that are configured for Q-signaling (QSIG) with gateways in between, the second setup message (which is a signal only) does not pass the correct information to the far-end PBX and causes the call to fail.

  Conditions This symptom is observed on a Cisco 2600 series router.

  Workaround There is no workaround.

  There is no workaround.

- CSCdw14064

  Symptoms A Cisco 3640 router may reload with a bus error.

  Conditions This symptom is observed on a Cisco 3640 router that is running Cisco IOS Release 12.2(6) and that has an ISDN interface that is configured using the **isdn protocol-emulate network** interface configuration command.

  Workaround There is no workaround.

- CSCdw16205

  A router may reload at the dialer_pending process. There is no workaround.

- CSCdw16210

  In a setup in which a Dialer Watch is used together with a Multilink PPP (MLP), a dialer profile, and an ISDN backup (with multiple BRI channels in the bundle), and if more than one link is in the multilink bundle, the Dialer Watch disconnects the dialer link if the idle timeout and the dialer watch disable timer expires. This behavior occurs even though the dialer watch reports that the primary interface is in the “DOWN” state. A new dialer call subsequently opens the primary link backup

again. This process repeats itself as long as the primary link is down. Everything works normally if multilink is enabled and if there is only one link allowed in the bundle. The Dialer Watch checks the primary link after the idle timeout but does not disconnect the backup link. There is no workaround.

- CSCdw16602

  Cisco IOS software will release a call after the software receives an ISDN disconnect with cause=user busy. There is no workaround.

- CSCdw20362

  A vendor-specific feature is not forced on a PPP user that is configured with a callback dialstring that is not null. This behavior occurs if this callback control protocol feature is not negotiated by the client during Link Control Protocol (LCP) negotiation and if the Challenge Handshake Authentication Protocol (CHAP) or the Password Authentication Protocol (PAP) is negotiated.

  Workaround: Configure the network access server (NAS) to refuse further caller authentication requests while the NAS is still authenticating other callers by issuing the **ppp chap refuse callin** interface configuration command and the **ppp pap refuse callin** interface configuration command.

- CSCdw20899

  On a router that is running Cisco IOS Release 12.2(6.6) or a later release, if a Network Control Program (NCP) is configured and then unconfigured on an interface that is in the "up" state, PPP will enter the "Terminating" state and no subsequent NCPs can be configured until the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command is entered on the interface.

  Workaround: Configure NCPs on the interfaces before bringing them up.

  Alternate workaround: Use Cisco IOS Release 12.2(7.4), 12.2(7.4)T, or a later release.

- CSCdw23757

  A Cisco 800 router may reload if a plain old telephone service (POTs) is off hook. This condition occurs when the **isdn switch-type** *switch-type* interface configuration command is configured. There is no workaround.

- CSCdw26352

  Symptoms An input queue on an virtual access interface may become wedged. This condition may cause the line to be dropped.

  Conditions This symptom is observed on a Cisco 1417 router that has a PPP over ATM (PPPoA) configuration that uses a virtual template interface.

  Workaround There is no workaround.

- CSCdw26515

  Symptoms A Cisco 7500 series router may reload with a bus error because of the following corrupted program counter (PC) in the dialer code:

  ```
  %ALIGN-1-FATAL: Corrupted program counter pc=0x10009, ra=0x10009, sp=0x62DB13D8
  ```

  Conditions This symptom is observed on a Cisco 7500 series router that is configured with a Route Switch Processor 4 (RSP4) when it is running an experimental image that is based on Cisco IOS Release 12.2(6.6)T.

  Workaround There is no workaround.

- CSCdw31797

  Symptoms A Cisco AS5400 reloads when a client that is using a third-party ISDN adapter attempts to add a second link using Bandwidth Allocation Protocol (BAP).

Conditions This symptom is observed when the Cisco AS5400 has the **ppp bap call accept acknowledge** command configured and the **debug ppp negotiation** command or the **debug ppp bap negotiation** command enabled.

Workaround Disable the debug commands.

- CSCdw38663

  A Cisco router may display a traceback message at the propagate_hunt_rprofile_changes() function when a configuration is changed on the dialer interface. There is no workaround.

- CSCdw38997

  Symptoms While a Cisco router is handling X.25 calls, several spurious accesses may occur. Errors such as the following may be displayed in the log:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x61233060 reading 0xAB
  %ALIGN-3-TRACE: -Traceback= 61233060 60943D34 6091039C 609104E8 60943DF4 60943F0C
  60949B48 60949B00
  ```

  A summary of the errors may be displayed by entering the **show alignment** privileged EXEC command:

  ```
  No alignment data has been recorded.
   Total Spurious Accesses 237, Recorded 4
     Address  Count  Traceback
          AB     79  0x61276A90 0x6096B444 0x60937304 0x60937450
                     0x6096B504 0x6096B61C 0x6097114C 0x60971104
          AB     79  0x61276A98 0x6096B444 0x60937304 0x60937450
                     0x6096B504 0x6096B61C 0x6097114C 0x60971104
          C0     78  0x6096B44C 0x60937304 0x60937450 0x6096B504
                     0x6096B61C 0x6097114C 0x60971104 0x60970BDC
          AB      1  0x61276AA4 0x6096B444 0x60937304 0x60937450
                     0x6096B504 0x6096B61C 0x6097114C 0x60971104
  ```

  Conditions This symptom is observed on a Cisco router that is running Cisco IOS Release 12.1(12) or an earlier release.

  Workaround There is no workaround.

- CSCdw44093

  Symptoms A Cisco AS5300may reload at the historyQinsert MIB after a call is made.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw50476

  Symptoms A call is rejected because a display information element (IE) is added to a Q.931 setup packet.

  Conditions This symptom is observed under the following conditions:

  When a call is received from a vendor-specific client, user information that is included in the H.225 call setup packet is forwarded to a class 5 switch in the form of a Q.931 packet that is filled with a display IE that is converted from the user information. However, the Q.931 standard reads the Q.931 packet as if it was sent only from the network side to the user side and the class 5 switch rejects the call. The display IE should not be included in the setup packet when a Cisco AS5300 is set as the user side by default.

  Workaround There is no workaround.

- CSCdw51944

  Symptoms IP connectivity may get lost and is then reestablished on a router. This situation causes packets that are coming from the router to have TCP checksum failures, and the packets are dropped.

  Conditions This symptom is observed when a serial tunnel is connected from a Cisco 7200 series router that is running Cisco IOS Release 12.2(7.5) to another router over a Voice over Frame Relay (VoFR) link.

  Workaround Reset the serial tunnel connection.

- CSCdw52524

  A Cisco 7200 router may reload if the **debug all** EXEC command followed by the **no debug all** EXEC command is entered on the router.

  Workaround: Enable each debug command separately on the router.

- CSCdw52712

  Symptoms An ISDN Layer 2 does not come up after a very short failure.

  Conditions This symptom is observed in a Signaling System 7 (SS7) environment, when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a serial interface and an ISDN Layer 2 fails.

  Workaround There is no workaround.

- CSCdw54250

  Symptoms Downstream Systems Network Architecture Switching Services (SNASw) users may experience session disconnects.

  Conditions This symptom is observed when the users are connecting to the SNA switch port that is an ATM LAN Emulation (LANE) subinterface. This behavior occurs when a router is running Portable SNA (PSNA) Advanced Peer-to-Peer Networking (APPN) software. This behavior may also occur when a router is running just PSNA.

  Workaround There is no workaround.

- CSCdw56892

  Symptoms The following error message is generated on a Cisco 7200 series router:

  ```
  ISDN Se2/0:15: Error: CALL_FAC_INV: no chan for call id 0xE80A found
  ```

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw57903

  Symptoms A Cisco AS5300 may reload when you configure the controller for the primary Non-Facility Associated Signaling (NFAS) channel and its D channel.

  Conditions This symptom is observed on a Cisco AS5300 that is running the c5300-js-mz image of Cisco IOS Release 12.2(7.4).

  Workaround There is no workaround.

- CSCdw58159

  Symptoms A Cisco AS5300 responds with a “Release complete” message with a cause code of 0xD1 (invalid call reference value).

  Conditions This symptom is observed when a 4 Electronic Switching System (4ESS) sends a setup message followed by a facility message.

  Workaround There is no workaround.

- CSCdw61367

  Symptoms Layer 2 Tunnel Protocol (L2TP) dial-out on an asynchronous link between a client and an L2TP access concentrator (LAC) may fail.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCdw62064

  Symptoms Inbound data packets that are reassembled from multilink fragments may not be processed properly on Multilink PPP (MLP) interfaces that are receiving encrypted IP Security (IPSec) traffic that is terminated locally when a hardware accelerator is used for decryption.

  Conditions This symptom affects all inbound reassembled data frames that are received by the bundle and not just those data frames that are carrying encrypted IP datagrams. Most significantly, inbound Internet Security Association and Key Management Protocol (ISAKMP) keepalives are not processed, leading to the eventual failures of the associated IPSec sessions.

  The IPSec sessions are reestablished after each failure, but traffic drops will occur until the session is renegotiated via the Internet Key Exchange (IKE). Thus, the observable symptoms are an intermittent failure of IPSec sessions combined with high loss rates in the encrypted data traffic.

  Workaround Disable hardware crypto acceleration, and use software crypto acceleration instead.

- CSCdw68465

  Symptoms A Cisco 6400 Node Route Processor 1 (NRP-1) may reload with one of the following messages:

  ```
  %SYS-3-OVERRUN: Block overrun at 6228DFC8 (red zone 0D0D0D0D)
  ```

  or

  ```
  %SYS-3-BADBLOCK: Bad block pointer 6252A6B0
  ```

  or

  ```
  %SYS-6-BLKINFO: 0x61FEB4C8 poison over FREEMAGIC 0x61FEB4C8
  ```

  Conditions This symptom is observed on rare occasions when memory corruption is caused because of Virtual Private Dialup Network (VPDN) session establishment failures that occur because session limits are exceeded, for example, when session limits are enforced by the **pppoe limit per-mac** VPDN configuration command or the **pppoe limit per-vc** VPDN configuration command.

  Workaround To prevent memory corruption, enter the **no vpdn history failure** hidden global configuration command, as in the following example:

  ```
  vpdn enable no vpdn history failure
  ```

  When you enter the **show running-config** EXEC command, the hidden command will be visible.

- CSCdw70675

  Symptoms A Cisco router may reload when dialer profiles are used to get links up to the destination with a Multilink PPP (MLP) configuration.

  Conditions This symptom is observed when there is an idle timeout or the dialer profile interface is disconnected.

  Workaround Use a rotary configuration instead of a dialer profile configuration.

- CSCdw71382

  Symptoms The output of the **show isdn nfas group** EXEC command shows an incorrect number for the total number of Non-Facility Associated Signaling (NFAS) members. This situation does not impair the system functionality.

Conditions The conditions under which this symptom occurs are not known at this time.

Workaround There is no workaround.

- CSCdw71445

  Symptoms A packet is incorrectly dropped by a router.

  Conditions This symptom is observed when a Frame Relay-encapsulated packet is a Multiprotocol Label Switching (MPLS) packet on locally switched Frame Relay permanent virtual circuits (PVCs) that are configured with the **connect** global configuration command or the **frame-relay route** interface configuration command. This condition affects only the Cisco 7500 series routers and only the Cisco IOS images that support MPLS switching, such as the rsp-pv-mz or rsp-jsv-mz image.

  Workaround There is no workaround.

- CSCdw76783

  Symptoms A Q.931 ISDN setup message with a terminal endpoint identifier (TEI) value of 127 (indicating that any TEI value available can be assigned) may be sent, despite a static TEI assignment.

  Conditions This symptom is observed on a Cisco router that is configured with an ISDN BRI/NT/TE voice interface card (VIC-2BRI-NT/TE) on the network side with a TEI that is statically assigned to zero.

  Workaround There is no workaround.

- CSCdw77025

  Symptoms Layer 2 Tunneling Protocol (L2TP) dial-out pings may fail.

  Conditions This symptom is observed when the dialer traffic originates from a Virtual Private Network (VPN) routing/forwarding instance (VRF).

  Workaround There is no workaround.

- CSCdw77931

  Symptoms When you originate a Voice over IP (VoIP) call to a busy user in the public switched telephone network (PSTN) via a BRI voice interface card (VIC-BRI), you cannot hear the busy tone from the PSTN and the call is unexpectedly terminated.

  Conditions This symptom is observed on a Cisco 3640 that is configured with a VIC-BRI and that is running Cisco IOS Release 12.2(7), Release 12.2(7.5), or Release 12.2(7.5)T. Note that the symptom does not occur on router that is configured with a PRI interface.

  Workaround There is no workaround.

- CSCdw82459

  Symptoms A router may reload when a Point-to-Point Tunneling Protocol (PPTP) tunnel is terminated.

  Conditions This symptom is observed on a router that has 128-bit encryption enabled when a PPTP tunnel is terminated because the router receives a packet that is larger than expected.

  Workaround Disable the 128-bit encryption.

- CSCdw91219

  Symptoms A router does not send a “release complete” message when a second T303 timer expiration occurs.

  Conditions This symptom is observed in a BRI NET3 switch type configuration.

  Workaround There is no workaround.

- CSCdx23889

  Symptoms Calls may be rejected when a gateway performs overlap sending such as in calls in which the called party number exceeds 20 digits.

  Conditions This symptom is observed on a gateway when the gateway uses overlap sending. The gateway rejects the call if a call proceeding message is received without a channel identity (ID) even though a channel ID has already been received in a setup acknowledgement message and a channel ID is not required.

  Workaround There is no workaround.

- CSCin01781

  Symptoms Call waiting does not function when the second call is an external call. It functions normally when the second call is an internal call.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.

- CSCin04769

  Symptoms A universal access sever may reload while it attempts to call another universal access server.

  Conditions This symptom is observed on a Cisco AS5300 universal access server that is running the c5300-js-mz.122-2.XB image of Cisco IOS Release 12.2(2)XB. This symptom occurs when the Cisco AS5300 initiates a V.110 call to a Cisco 5850 universal access server.

  Workaround There is no workaround.

- CSCin05568

  Symptoms A router may reload after the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command is entered on an interface.

  Conditions This symptom is observed on an X.25 over an ISDN D-channel interface. This symptom occurs after the **shutdown** interface configuration command is entered and when the **no shutdown** interface configuration command is entered on the interface after the timer is started. This symptom occurs only if X.25 is configured on the interface.

  Workaround There is no workaround.

- CSCuk30274

  Symptoms A protocol emulate network cannot be configured for the NET 5 switch type.

  Conditions The conditions under which this symptom occurs are not known at this time.

  Workaround There is no workaround.