# Release Notes for Cisco 3200 Series Routers with Cisco IOS Release 12.4(11)XW

**First Released: August 12, 2008**
**Last Revised: February 5, 2009**
**Cisco IOS Release 12.4(11)XW10**
**OL-17636-02 Second Release**

These release notes describe new features and significant software components for the Cisco 3200 series routers in the Cisco IOS Release12.4(11)XW releases. These release notes are updated as needed. Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.4T* and *About Cisco IOS Release Notes*.

For a list of the software caveats that apply to the Release 12.4(11)XW releases, see the "Caveats" section on page 4, and the online *Caveats for Cisco IOS Release 12.4T*. The caveats document is updated for every 12.4T maintenance release.

# Contents

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

# System Requirements

This section describes system requirements for Cisco IOS Release 12.4(11)XW and includes the following sections:

## Memory Requirements

Table 1 lists memory requirements for Cisco IOS feature sets supported by Cisco IOS Release 12.4(11)XW on Cisco 3200 series routers.

***Table 1 Memory Requirements for Cisco 3200 Series Routers***

| Platform | Feature Set | Image | Flash Memory (MB) | RAM Memory (MB) |
|---|---|---|---|---|
| Cisco 3220 | Advanced Enterprise | c3220-adventerprisek9-mz | 32 | 128 |
| Cisco 3250 | Enterprise Base | c3250-entbase-mz | 64 | 192 |
| Cisco 3250 | Advanced Enterprise | c3250-adventerprisek9-mz | 64 | 192 |
| Cisco 3270 | Advanced Enterprise | c3270-adventerprisek9-mz | 64 | 256 |
| Cisco 3270 | Enterprise Base | c3270-entbase-mz | 64 | 256 |

## Hardware Supported

Cisco IOS Release 12.4(11)XW supports the following Cisco 3200 series routers:

- Cisco 3220
- Cisco 3250
- Cisco 3270

For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 3200 series routers, which are available at

http://www.cisco.com/en/US/products/hw/routers/ps272/tsd_products_support_series_home.html

## Determining the Software Version

To determine the version of Cisco IOS software currently running on your Cisco 3200 series router, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

## Upgrading to a New Software Release

For general information about upgrading to a new software release, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

## Feature Set Tables

For information about feature set tables, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

# New and Changed Information

The following sections describe new features supported by Cisco 3200 series routers in Cisco IOS Release 12.4(11)XW:

## New Hardware Features in Cisco IOS Release 12.4(11)XW10

There are no new hardware features in this release.

## New Software Features in Cisco IOS Release 12.4(11)XW10

There are no new software features in this release.

## New Hardware Features in Cisco IOS Release 12.4(11)XW9

There are no new hardware features in this release.

## New Software Features in Cisco IOS Release 12.4(11)XW9

There are no new software features in this release.

## New Software Features in Cisco IOS Release 12.4T

For information regarding the features supported in Cisco IOS Release 12.4T, see the *Cross-Platform Release Notes* links at: http://www.cisco.com/en/US/products/ps6441/prod_release_notes_list.html

# Limitations and Restrictions

There are no known limitations or restrictions in this release.

# Caveats

For general information on caveats and the bug toolkit, see *About Cisco IOS Release Notes* located at http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html.

This section contains the following caveat information:

## Open Caveats - Cisco IOS Release 12.4(11)XW10

There are no open caveats in this release.

## Resolved Caveats - Cisco IOS Release 12.4(11)XW10

- CSCsv04836

  Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

  In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

  Cisco has released free software updates for download from the Cisco website that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090908-tcp24.shtml.

- CSCsm27071

  A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

  - The configured feature may stop accepting new connections or sessions.

  - The memory of the device may be consumed.
  - The device may experience prolonged high CPU utilization.
  - The device may reload. Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory. The advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml

- CSCsm97220

  Devices that are running Cisco IOS Software and configured for Mobile IP Network Address Translation (NAT) Traversal feature or Mobile IPv6 are vulnerable to a denial of service (DoS) attack that may result in a blocked interface.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at the following link
  http://www.cisco.com/warp/public/707/cisco-sa-20090325-mobileip.shtml

- CSCso05337

  Devices that are running Cisco IOS Software and configured for Mobile IP Network Address Translation (NAT) Traversal feature or Mobile IPv6 are vulnerable to a denial of service (DoS) attack that may result in a blocked interface.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at the following link
  http://www.cisco.com/warp/public/707/cisco-sa-20090325-mobileip.shtml

- CSCsv38166

  The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

  The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS SCP client feature.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml.

- CSCsu11522

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS software that can be exploited remotely to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address this vulnerability. There are no workarounds available to mitigate the vulnerability apart from disabling SIP, if the Cisco IOS device does not need to run SIP for VoIP services. However, mitigation techniques are available to help limit exposure to the vulnerability.

This advisory is posted at the following link:

http://www.cisco.com/warp/public/707/cisco-sa-20090325-sip.shtml.

- CSCsk64158

  Symptoms: Several features within Cisco IOS software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory. This advisory is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml.

- CSCsw24700

  Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

  1. Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.
  2. SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds that mitigate these vulnerabilities. This advisory is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml

- CSCso04657

  Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

  Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If "debug ip tcp transactions" is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.

```
CSCin76666 H.245 listener socket closed before H.245 connection is established.
```

**Symptom** Intermittent outbound call failures using CallManager and Outbound Fast Start.

**Conditions** CallManager receives an inbound H.225 Facility message with startH245 at the same time as CCM transmits an H.225 Facility message with startH245. CCM closes the outbound H.245 TCP socket per H.323 Spec. Because the GW also closed the H.245 TCP socket it created, H.245 negotiation will halt and the call will fail.

**Workaround** Disable outbound fast start and this problem will not occur.

```
CSCse59336 Three way call conferencing is not working properly.
```

**Symptom** MGCP three-way call conferencing may fail because of an abrupt onhook event at the originating endpoint.

**Conditions** This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(9.13) and that is configured for voice calls over the Media Gateway Control Protocol (XGCP).

**Workaround** None.

```
CSCsg35148 Interim record is sent with stop-only acct-list from RADIUS.
```

**Symptom** Interim record is seen.

**Conditions** Conditions:stop-only ppp-acct-list is downloaded from merit RADIUS server.

**Workaround** None.

```
CSCsi95862 3250 router crashes with traceback while verifying gre feature.
```

**Symptom** Router crashes when the **<CmdBold> mobile router-service roam priority <noCmdBold>** command is entered.

**Conditions** Crash is observed during unconfiguration after verifying for generic routing encapsulation.

**Workaround** None.

```
CSCsj04758 Wrong codec bytes on the SIP leg of ipipgw for SIP--->H323 (g726).
```

**Symptom** Wrong codec bytes are displayed on the SIP leg of ipipgw for SIP--->H323 interworking.

**Conditions** Work codec bytes of "0" is seen when SIP--->H323 interworking is done when codec g726 codec is configured. Call goes through fine but wrong bytes are displayed.

**Workaround** None.

```
CSCsj75250 crafted SCTP packet reloads router.
```

**Symptom** Crafted SCTP packet may reset router.

**Conditions** Affects Cisco IOS devices running 12.4(15)T and later based trains.

**Workaround** If not using SCTP on the device an infrastructure ACL, denying SCTP traffic to the device can be applied inbound to all interfaces.

```
CSCsk40676 C1812 12.4.15.T / certain packet sizes block inside interface of ezvpn
conn.
```

**Symptom** The inside interface of a Cisco router running EZVPN may become unresponsive when sending ICMP messages from a remote VPN client connection.

**Conditions** Occurs when LZS compression is used on a Windows Vista client.

**Workaround** Disable LZS compression.

```
CSCsm45113 RIB installs duplicate routes for the same prefix
```

**Symptom** Router may install duplicate routes or incorrect route netmask into routing table. It could happen on any routing protocol. Additionally, for OSPF, crash was observed.

**Conditions** The problem is triggered by SNMP polling of ipRouteTable MIB. The problem is introduced by CSCsj50773, see the Integrated-in field of CSCsj50773 for affected images.

**Workaround** Do not poll ipRouteTable MIB, poll newer replacement ipForward MIB. instead. The ipRouteTable MIB was replaced by ipForward MIB in RFC 1354.

**Further Problem Description:** The <CmdBold>clear ip route *<noCmdBold> command can correct the routing table until the next poll of ipRouteTable MIB.

```
CSCsm49826 c7206VXR/NPE400 reloaded due to bus error running 12.4(15)T2 and T3.
```

**Symptom** H323 gateways crash under load.

**Conditions** Multiple H323 calls were made simultaneously.

**Workaround** Configuring the following CLI should prevent the crash:

```
c2691-15(config)#voice service voip
c2691-15(conf-voi-serv)#h323
c2691-15(conf-serv-h323)#no h245 simultaneous-connection-handle
```

```
CSCso47738 No Voice Path For SIP to H323 calls.
```

**Symptom** Gateway sends 200 OK with media direction as SENDRECV for a reINVITE with offer having media direction INACTIVE.

**Conditions** This is seen for the supplementary services when the call is put on HOLD and then RESUMED.

**Workaround** None.

```
CSCso80830 W button should be lit on for undefined primary ephone.
```

**Symptom** The Watch button is not lit on if no watched phone for this watched DN. Ring back tone is heard when calling to this DN.

**Conditions** No phone, no matter registered or not, is configred with the watched DN.

**Workaround** None.

```
CSCsq04046 GUI: IOS SYSfeature undefined" error seen on help->about.
```

**Symptom** Error when accessing CME GUI Help->About page.

**Conditions** Using IOS image with feature variable more than 50 characters.

**Workaround** None.

```
CSCsr27960 Traceback observed after configuring credential under sip-ua.
```

**Symptom** Traceback observed when configuring credentials CLI under sip-ua.

**Conditions** This happens when user configures credentials CLI with username length more than 32 characters.

**Workaround** None.

```
CSCsr78883 Router console displays messages "Data corruption Data Inconsistency.
```

**Symptom** There will be traceback on configuring **mls qos cos pass-through dscp** in supporting interface mode.

**Conditions** Configuring "mls qos cos pass-through dscp" in the interface that supports the functionality.

**Workaround** Currently, the CLI is not supported in most network modules, and thus, is invisible to the users. If the CLI is supported, configure it as **mls qos cos override | cos-value** </B>

**Further Problem Description:** Due to the buffer overflow, there will be traceback when configuring the QoS in the supporting interface. Currently, the CLI is not supported in most network modules, and thus,is invisible to the users.

```
CSCsu36827 CUE clock does not sync up with the CME using NTP.
```

**Symptom** The CUE clock does not synch up with the CME using NTP.

**Conditions** This symptom is observed when the UC500 is configured as the NTP master.

**Workaround** Use an external NTP server other than the UC500.

```
CSCsu59847 The Content-Type used by T.37 should use a mutipart subtype of "mixed".
```

**Symptom** Certain mail clients may experience problems viewing the TIFF attachments sent by a Cisco T.37 OnRamp gateway because they do not support the Content-Type of multipart/fax-message that Cisco uses in it's T.37 Store-and_forward Fax implementation.

**Conditions** This problem should not affect most mail clients because Cisco is not in violation of any specifications. The MIME specification (RFC2046) clearly states that a mail client should treat an unrecognized subtype of multipart as being equivalent to the well known and widely used Content-Type of multipart/mixed.

**Workaround** None.

```
CSCsw50802 Smart Init Fails to recognize HWICs with smart cookie.
```

**Symptom** No extra I/O mem is allocated for some HWICs.

**Conditions** When HWIC is equipped with smart cookie.

**Workaround** Using static I/O mem configuration instead.

## Open Caveats - Cisco IOS Release 12.4(11)XW9

There are no open caveats in this release.

## Resolved Caveats - Cisco IOS Release 12.4(11)XW9

CSCek52673 Single crafted udp packet reloads router with dhcp server

**Symptom** A router that has DHCP server enabled could reload after receiving a malformed UDP packet.

**Workaround** There is no workaround.

CSCek71149 Error message when **dir** is issued

**Symptom** "Error getting file system status (Unknown error 0) or (Bad file number)" was observed when **dir <archive/system/tmpsys:>** was issued. The rest of the file systems have no problem (i.e. **dir nvram/flash/usbtoken0:**... etc)

**Conditions** Load routers with problem releases.

**Workaround** There is no workaround.

CSCsg42546 Reload when MGCP CRCX has sRTP and V150 params in LCO

**Symptom** An MGCP gateway reloads when receiving Secure Real-Time Transport Protocol (SRTP) and V.150 parameters in the local connection options of a Create Connection (CRCX) message.

**Conditions** This symptom has been observed when the gateway is configured to use SRTP and V.150 protocols.

**Workaround** Disable the use of either SRTP or V.150 protocol in the gateway.

```
CSCsj32422 CBWFQ:Unable to reconfigure the policy map after exceeding the
bandwidth
```

**Symptom** Once policy map is configured and bandwidth is exceeded while dividing amongst the classes, re-configuration of the policy map is not possible.

**Conditions** Create a policy map, exceed the bandwidth amongst the classes (e.g. try to divide more than 75% in CBWFQ).

**Workaround** Don’t exceed the bandwidth while configuring the policy map.

```
CSCsj50773 High cpu when querying ipRouteTable MIB
```

**Symptom** Performing the snmpwalk on the ipRouteTable MIB may cause high CPU and reloads.

**Conditions** This symptom is observed on a router that is running Cisco IOS Release 12.4(13b) or later releases.

**Workaround** Create a view that excludes the ipRouteTable:

**snmp-server view cutdown 1.3.6.1.2.1.4.21 exclude**

**snmp-server view cutdown internet included**

**snmp-server community <comm> view cutdown RO**

This view restricts the objects that the NMS can poll. It excludes access to the ipRouteTable, but allows access to the other MIBs.

```
CSCsj82622 Crash editing ACL cce_dp_named_db_ip_access_list_impure
```

**Symptom** A router may crash when you configure an access control list (ACL) that has at least 50-60 ACEs (about 100 nodes) that is used in policy maps that are already applied to an interface or when you boot the router after having made the configuration change. When the crash occurs, the following error message is generated: %ALIGN-1-FATAL: Corrupted program counter pc=0x0 , ra=0x0 , sp=0x66EFB8A0

**Conditions** This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.4(15)T or Release 12.4(15)T1.

**Workaround** There is no workaround.

```
CSCsk27147 SNMP stops responding while polling from CISCO-MEMORYPOOL-MIB
```

**Symptom** The following SNMP is incorrectly generated:"%SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full”. This issue is affecting the CISCO-MEMORYPOOL-MIB instead.

**Conditions** Occurs on a Cisco 2600 series router running Cisco IOS Release 12.4(11)T3. The router keeps dropping SNMP packets. The log shows that the packets are dropped because of the input queue being full. Although the utilization is sometimes high, this could not be the root cause, as the router keeps dropping packets regardless of the current utilization. Also, the snmp process takes 5-20% of the CPU load.

**Workaround** Exclude ciscoMemoryPoolMIB from your query with the following commands:

**snmp-server view public-view iso included**

**snmp-server view public-view ciscoMemoryPoolMIB excluded.**

Apply this view to the RW community string. This view will exclude only ciscoMemoryPoolMib, all other MIBs will be available.

```
CSCsk39642 router crash when copying saved config to running config
```

**Symptom** A router crashes.

**Conditions** This symptom is observed when you are running Cisco IOS Release 12.4(17) or Release 12.4T and when you copy the saved configuration to the running configuration.

**Workaround** There is no workaround.

```
CSCsk94676 dlsw with tbridge, COMMON_FIB-4-FIBIDBMISMATCH
```

**Symptom** Transparent bridging into DLSw does not work.The following messages are displayed:

> *Jan 29 19:00:50.727: %COMMON_FIB-4-FIBHWIDBMISMATCH: Mis-match between hwidb DLSw Port0 (ifindex 5) and fibhwidb GigabitEthernet2/3 (ifindex 5)-Traceback= 407C7004 407C8A38 407C7CEC 407C7EE4 413C9900 41BCE138 41BCCD54 41BCCFA8 41BCA330 413C0128 413C0114
>
> *Jan 29 19:00:50.727: %COMMON_FIB-4-FIBMISSINGHWIDB: No fibhwidb while initializing fibidb for DLSw Port0 (if_number 5)
>
> -Traceback= 407C83D4 407C8A9C 407C7CEC 407C7EE4 413C9900 41BCE138 41BCCD54 41BCCFA8 41BCA330 413C0128 413C0114

**Conditions** When using DLSw+ together with transparent bridging.

**Workaround** For a workaround, all transparent bridging commands related to **dlsw** can be replaced with DLSW Ethernet redundancy.

i.e.

As global command:

**no dlsw bridge-group X**

and on the interface:

**no bridge-group X**

on the interface replace it with:

**dlsw transparent redundancy-enable 9999.9999.9999**

```
CSCsl70722 Router crash polling rttmon mib with active IP SLA probes
```

**Symptom** A router running Cisco IOS may crash due to watchdog timeout.

**Conditions** Occurs when IP SLA probes are configured and active for a period of 72 weeks. After this much time has passed, polling the rttmon mib for the probe statistics will cause the router to reload. Then the problem will not be seen again for another 72 weeks.

**Workaround** There is no workaround.

```
CSCsm17281 Router crashes when adding ACL line to Service Policy
```

**Symptom** Device running 12.4(17.6)T will crash after adding line to an access-list attached to a service policy

**Workaround** There is none.

```
CSCsm77199 DATACORRUPTION-1-DATAINCONSISTENCY HTTP_FIND_FLASH_FILE
```

**Symptom** If the HTTP secure server capability is present, Switch shows the error message "%DATACORRUPTION-1-DATAINCONSISTENCY: copy error" with tracebacks after initializing the supervisor. This error message can be verified in **show logging** output.

**Conditions** **ip http server** is configured.

**Workaround** Configure **no ip http server.** The switch functionality is not affected by this error message.The problem is cosmetic.

```
CSCso09539 ACK not sent to 200 OK from CUE during h323 slowstart -- sip delayed med
```

**Symptom** Incoming H323 slow start call to CME when forwarded to voicemail in CUE may result in no audio.

**Conditions** This problem was observed when CME did not send ACK to 200 OK response from CUE.

**Workaround** Use H323 Faststart.If incoming H323 calls need to be slow-start for video calls and calls to voicemail need to be faststart, enable H.450 call transfer feature and use two incoming dial-peers:

- One H323 dial-peer configured with "**incoming called-number <ephone-dn extension range>**" and H323 slowstart using voice-class h323.
- Another H323 dial-peer configured with "**incoming called-number <voicemail dn>**" and H323 faststart using voice-class h323.

```
CSCsq42134 JPN: 7921 XML Services are displayed as squares
```

**Symptom** 7921 directories are displayed as squires in CME Userlocale: JP environment.

**Conditions** 7921: 1.1.1

CME: 4.2 (IOS 12.4(11)XW7)

Locale File : CME-locale-jp_JP-4.1.0.1.tar

**Workaround** There is no workaround.

```
CSCsq44013 View used twice with logging enabled
```

**Symptom** The CPE does not reply to the DNS query from the client for the first try, first response is being dropped.

**Conditions** This is seen on a router running 12.4T IOS image configured with Split DNS

The view is used twice rather than once.

**Workaround** There is no workaround.

```
CSCsq64715 EM login credential could be set to stack junk in error condition
```

**Symptom** EM login username and password may be set to random values in process stack in case the actual input from the phone is in an invalid format. And if both string picked up from the stack happen to match a username/password pair in a configured user profile, EM will login the user accidentally.

**Workaround** There is no workaround.

```
CSCsq67163 IPSLA RTP operation crashes the router
```

**Symptom** Scheduling of IP SLA RTP operation crashes the router.

**Conditions** This problem occurs only when IPSLA RTP operation is configured and is scheduled to run.

**Workaround** There is no workaround.

```
CSCsq74999 SCCP FXS ports connected to FAX machines lock up
```

**Symptom** FXS that have fax/modems connected intermittently fail. Once they are in this stuck state, an incoming call to them will not ring the line, there will be no output in **debug vpm sig**. Outbound calls/faxes typically still work.

FXS port must be SCCP controlled. The problem is likely to occur when the pots leg is disconnected before the voip leg. If this occurs the port can go into this "stuck" state. Any subsequent calls will not ring the fax machine on this port.

**Workaround** Temporary workaround is to "shut/no shut" the voice-port. This problem seems to be related to cisco fax-relay being invoked and it's interoperability with SCCP in this IOS version. Configuring:

```
voice service voip
  fax protocol none
```

will prevent the problem from happening. Removing the SCCP config from the ports will also prevent it from happening.

```
CSCsr01058 SPLIT_DNS: Debug msg Forwarding back reply is missing
```

**Symptom** An IOS device configured as a DNS server is vulnerable to forged answer attacks. In this type of attack, a malicious user can cause the IOS DNS server to accept a forged answer that associates a name with an IP address chosen by the malicious user. This answer ends up in the cache of the DNS server. This attack can be made more difficult by randomizing both the DNS transaction ID and the UDP source port number that the DNS server (the IOS device) uses to relay DNS queries for domain it is not authorized for.

**Conditions** The above symptom is seen on a router loaded with 12.4(19.18)T image and above.

**Workaround** In the case of IOS, when the IOS name server relays a query, the DNS transaction ID that is used is the original ID received from the client, and the source UDP port is always 53. To make the IOS DNS server more resilient and less vulnerable to DNS cache poisoning attacks, at the very minimum both the DNS transaction ID and the UDP source port number must be randomized. The use of bit 0x20 in DNS labels to improve transaction identity is also recommended.

This is a security issue. The problem, however, only exists for customers who are running the IOS DNS Server/Forwarder and this is presumed to not be the usual case.

```
CSCsr18200 busy tone issue when receiving a 183 Message
```

**Symptom** A busy tone is not heard when a 183 message is received before a 4xx busy message.

**Conditions** SIP Trunk architecture with Italtel SSW. The bug affects both 12.4(15)T and 12.4(11)XW software releases.

**Workaround** A patch is required, forcing the media off when a busy message is received.

```
CSCsr71715 Call display missing when park or xfer HW conference call
```

**Symptom** Caller ID and Call bubble missing when a HW conference call is parked or Xfere

## Open Caveats - Cisco IOS Release 12.4(11)XW7

There are no open caveats in this release.

## Resolved Caveats - Cisco IOS Release 12.4(11)XW7

- CSCsk62253

  Cisco IOS software contains two vulnerabilities within the Cisco IOS WebVPN or Cisco IOS SSLVPN feature (SSLVPN) that can be remotely exploited without authentication to cause a denial of service condition. Both vulnerabilities affect both Cisco IOS WebVPN and Cisco IOS SSLVPN features:

  1. Crafted HTTPS packet will crash device - Cisco Bug ID CSCsk62253.
  2. SSLVPN sessions cause a memory leak in the device - Cisco Bug ID CSCsw24700.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds that mitigate these vulnerabilities. This advisory is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20090325-webvpn.shtml

# Additional References

Use this release note with the documents and websites in this release note and the documents listed in the following sections:

- Release-Specific Documents, page 19
- Platform-Specific Documents, page 19

## Release-Specific Documents

The following documents are specific to Release 12.4 and apply to Release 12.4(11)XW.

- *Cross-Platform Release Notes for Cisco IOS Release 12.4T*
- *Cisco IOS Software Releases 12.4 Special and Early Deployments*
- *Caveats for Cisco IOS Release 12.4(20)T*

## Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 3200 series routers are at

http://www.cisco.com/en/US/products/hw/routers/ps272/tsd_products_support_series_home.html

## Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents.

### Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference. *Cisco IOS Software Documentation* is available in html or pdf form.

Select your release and click the command references, configuration guides, or any other Cisco IOS documentation you need.

# Notices

See the “Notices” section in *About Cisco IOS Release Notes* located at

http://www.cisco.com/en/US/docs/ios/12_4/12_4x/12_4xy15/ReleaseNote.html

Use this document in conjunction with the documents listed in the “Additional References” section.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.