Release Notes for the Cisco 10000 Series Router for Cisco IOS Release 12.0(30)SZ4

Published: September 2008

These release notes provide information about Cisco IOS Release 12.0(30)SZ4 for the Cisco 10000 Series Router. This release is a maintenance release and has no new features.

For a list of the software caveats that apply to Cisco IOS Release 12.0(30)SZ4, see the "Caveats for Cisco IOS Release 12.0(30)SZ4" section on page 4.

Cisco IOS Release 12.0(30)SZ4 is based on the following releases:

- Cisco IOS Release 12.0(30)S5
- Cisco IOS Release 12.0(30)SZ through Release 12.0(30)SZ3

To review the release notes for Cisco IOS Release 12.0 S, go to the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/prod_release_notes_list.html

Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/tech_tips/index/fn.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/tech_tips/index/fn.htm

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

Contents

These release notes describe the following topics:

System Requirements

The following sections describe the system requirements for Cisco IOS Release 12.0(30)SZ4:

Supported Hardware

For Cisco IOS Release 12.0(30)SZ4, you must have the performance routing engine (PRE), Part Number ESR-PRE1 installed in the Cisco 10000 series chassis. To verify which PRE is installed in the router, use the **show version** command.

For information about line cards supported by Cisco 10000 series routers, see the "Supported Line Cards for the 10000 Series Routers" section in the *Cross-Platform Release Notes for Cisco IOS Release 12.0 S, Part 1: System Requirements*, located at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/prod_release_note09186a00803c2dcb.html

Feature Support

Cisco IOS software is packaged in feature sets, depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Cisco IOS Release 12.0(30)SZ4 is based on Cisco IOS Release 12.0(30)S5 and subsequent Cisco IOS Release 12.0(30)SZ*x* maintenance releases. All features supported by Cisco IOS Release 12.0S up to and including Release 12.0(30)S5 are supported by Cisco IOS Release 12.0(30)SZ4.

Caution Cisco IOS images with strong encryption (including, but not limited to, 168-bit Triple Data Encryption Standard [3DES] data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of United States government regulations. When applicable, purchaser and user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Upgrading to a New Software Release

The following sections provide information about upgrading your Cisco 10000 series router to a new software release:

Before You Upgrade the Cisco IOS Software

Before you upgrade (or downgrade) the Cisco IOS software running on the Cisco 10000 series router, save the running configuration file using the **copy** command. In route processor redundancy (RPR) mode, the router synchronizes only the startup configuration.

Information About Upgrading to a New Software Release

For specific information about upgrading your Cisco 10000 series router to a new software release, see the *Cisco 10000 Series Router Performance Routing Engine Installation*, located at the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps133/prod_installation_guide09186a0080525aba.html

For general information about upgrading to a new software release, see the product bulletin *Cisco IOS Upgrade Ordering Instructions*, located at the following URL:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm#wp26467

For additional information about ordering Cisco IOS software, see the Products and Services Ordering web site, located at the following URL:

http://www.cisco.com/en/US/ordering/index.shtml

New and Changed Features

The following sections list the new and changed hardware and software features supported by Cisco 10000 series routers:

New Features—Cisco IOS Release 12.0(30)SZ4

Cisco IOS Release 12.0(30)SZ4 is a maintenance release and has no new hardware or software features.

For information about new features supported on the Cisco 10000 series router in other releases, see the appropriate Release Notes, located at the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps133/prod_release_notes_list.html

New Features—Cisco IOS Release 12.0(30)S5

Cisco IOS Release 12.0(30)S5 has no new hardware or software features.

For information about Cisco IOS Release 12.0(30)S releases, see the appropriate document, located at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/prod_release_notes_list.html

Important Notes

The following sections provide important information for your review:

- Inserting a New Line Card, page 4
- Deferral of Cisco IOS Software Images, page 4

Inserting a New Line Card

Unlike other Cisco routers, if you insert a new or different line card into a Cisco 10000 series chassis slot that previously had a line card installed, the line card initially reports that it is administratively up.

Deferral of Cisco IOS Software Images

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices located at the following URL to determine if your software release is affected:

http://www.cisco.com/kobayashi/sw-center/sw-ios-advisories.shtml

Caveats for Cisco IOS Release 12.0(30)SZ4

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats and only select severity 3 caveats are included in the caveats section of this document.

Cisco IOS Release 12.0(30)SZ4 is based on Cisco IOS Release 12.0(30)S5 and Releases 12.0(30)SZ through 12.0(30)SZ3, and contains all of the open caveats and fixes in these releases.

For information on the caveats in Cisco IOS Release 12.0(30)S5, see the *Cross-Platform Release Notes for Cisco IOS Release 12.0 S, Part 3: Caveats for 12.0(30)S through 12.0(32)S6*, located at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1829/prod_release_note09186a00803c2609.html

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.2 > Troubleshooting > Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you request is not displayed, it might be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

The following sections describe open and resolved caveats for the following maintenance release:

Open Caveats—Cisco IOS Release 12.0(30)SZ4

This section describes caveats that are open in Cisco IOS Release 12.0(30)SZ4.

CSCdy45049

During a lab stress test, line rate traffic sometimes does not achieve line rate when scaling over 3000 serial interfaces. This occurs only when thousands of serial interfaces with PPP or HDLC encapsulation are used on the port and line rate traffic is sent through all interfaces.

Workaround: No workaround is available.

CSCeh48414

While testing the high availability (HA) Stateful Switchover (SSO) feature, the traffic is not stable before or after the switchover occurs. This behavior occurs on a Cisco 10000 series router with 200 serial network interfaces, two channelized OC-12 interfaces, and one Ethernet interface. The problem is observed on the 200 interfaces and only when the router is running Cisco IOS Release 12.0(25)SX10.

Workaround: No workaround is available.

CSCeh73497

After a route processor (RP) switchover, the following message is sometimes observed. This occurs on the Cisco 10000 series router with redundant PRE1 cards and with RPR+ mode configured.

```
C10KEVENTMGR-1-IRONBUS_FAULT: Barium Error
```

The message results from an internal timing issue during the RP switchover. The affected line card recovers successfully and no performance impact is observed.

Workaround: No workaround is available.

CSCei54595

Unframed E1s with SONET VT framing show a high throughput loss. This occurs when the router is running Cisco IOS Release 12.0(28)S3 and affects the 1-port channelized OC-12/STM-4 and 4-port channelized OC-3/STM-1 line cards.

Workaround: An unframed E1 uses all 32 available channel groups, but a framed E1 might use up to 31 channels with the last channel reserved for framing bits. Because the framed E1s do not show the same performance loss, a possible workaround is to utilize the framed E1s with 31 channels.

CSCei93434

While configuring high availability (HA) Multilink, a slight buffer leak is observed after issuing the **show hardware pxf cpu buffers** command. As shown in the following sample output, for buffer pool 3 the total number of buffers (67666) does not equal the number of available buffers (67139). This occurs when the router is running Cisco IOS Release 12.0(28)S4.

```
 pool    size    # buffer    available   allocate failures
-----------------------------------------------------------
 0       9216    100            100         0
 1       4672    500            500         0
 2       1600    30000          30000       0
 3       640     67666          67139       0
 4       256     98165          98165       0
 5       64      131000         131000      0
```

Workaround: No workaround is available.

CSCej89322

Spurious memory access is observed at fib_notify_interface_state_change after the secondary switchover in the primary router. This symptom occurs on the router when running Cisco IOS Release 12.0(30)S4 and Release 12.0(28)S5.

Workaround: No workaround is available.

CSCsg51693

A random ping failure occurs between two CE routers and is randomly observed across different virtual private networks (VPNs) for more than 300 VPNs. The number of ping failures across the VPNs varies randomly. The number of VPNs is set to 500 and the number of VPN routes is set to 136. Ping operations between two PE routers works fine. The ping failure is not observed when the number of VPN routes is set to 0 and the number of VPNs is set to 999. This symptom occurs when the router is running Cisco IOS Release 12.0(30)SZ and Release 12.0(30)SZ2.

Workaround: No workaround is available.

Resolved Caveats—Cisco IOS Release 12.0(30)SZ4

This section describes caveats that were fixed in Cisco IOS Release 12.0(30)SZ4.

Cisco IOS Release 12.0(30)SZ4 is based on Cisco IOS Release12.0(30)SZ3 and contains the hardware and software features, and caveats included in Release 12.0(30)SZ3.

For information about caveats fixed in other Cisco IOS releases, refer to the appropriate Release Note document at the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps133/prod_release_notes_list.html

CSCdu73495

Enhanced Interior Gateway Routing Protocol (EIGRP) routes could not be seen even when the message digest algorithm 5 (MD5) was authenticated on all routers. This problem was intermittent and occurred when authentication was turned off and subsequently turned back on again. Sometimes, this problem occurred just after authentication was enabled. This has been fixed.

CSCeh88455

High CPU utilization occurred due to a SuperACL process after a named ACL change. Any named ACL change caused all QoS policies to be recompiled, except the policy maps that were only using that named ACL. This has been fixed.

CSCei45669

An OSPF router sometimes updated and originated a new version of a Link State Advertisement (LSA) when it should have flushed the LSA. This was observed on the originating router when it received a self-originated MaxAge LSA before it flushed this LSA from its database. This symptom occurred under a rare condition when a neighboring router calculated that it had a newer copy of the LSA from the originating router and bounded the MaxAge LSA to the originating router. This has been fixed.

CSCek51990

When the router was running the Cisco IOS 12.3(7)XI8b software image, the configured interfaces on the 1-port channelized OC-12 line card with E1/SDH framing took longer to come up and stabilize than they took when running the Cisco IOS 12.2(7)XI8a image. The interfaces took at least two to three minutes longer to come up due to the resolution of CSCse73990. This occurred when the line card was fully scaled (for example, 768 interfaces). When the router had fewer interfaces configured, the expected time to come up was less. This has been fixed.

CSCin78811

The slave Route Switch Processor (RSP) reloaded if a new multilink bundle was configured. This occurred on a Cisco 7500 series router with dual RSPs and running Cisco IOS Release 12.0(24)S6. This has been fixed.

CSCin98792

On the Cisco 10000 series router, issuing the **show running-config** or **show tech** command immediately after the **write memory** command sometimes resulted in a PRE failure. This behavior was more likely to occur when dual (redundant) PREs were configured on the router. This has been fixed.

CSCsd95616

Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates 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-20080924-multicast.shtml.

CSCsg15342

Cisco 10000, uBR10012 and uBR7200 series devices use a User Datagram Protocol (UDP) based Inter-Process Communication (IPC) channel that is externally reachable. An attacker could exploit this vulnerability to cause a denial of service (DoS) condition on affected devices. No other platforms are affected.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-ipc.shtml.

CSCsh77441

The switchover convergence time was greater than expected for Stateful Switchover (SSO) mode. The actual convergence time was greater than 10 seconds for HA SSO, while the expected time for convergence was 10 seconds. This occurred on a router running Cisco IOS Release 12.0(30)SZ. This has been fixed.

CSCsh83540

The PXF failed during MPLS precedence testing and a traceback message was observed after the PXF reloaded. This occurred when the **bump inhibit** command was configured on a VC and an IP packet did not have a PVC through which to flow. This has been fixed.

CSCsi01470

A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml.

CSCsi45417

After removing and re-adding the multilink PPP (MLPPP) group on a MLPPP bundle serial interface, the bundle ID was not copied to the standby PRE. This condition caused MLPPP to fail after a PRE switchover because the standby PRE did not accept the new command. This behavior occurred on a Cisco 10000 series router running Cisco IOS Release 12.0(28)S, Release 12.0(30)S, and Release 12.0(20)SZ and later releases, and with redundant PRE1s configured for stateful switchover (SSO) mode. This behavior was observed only on the serial interfaces of the 24-port channelized T1/E1 line card. Other line cards were not affected. This has been fixed.

CSCsi66221

When a multirouter automatic protection system (MR-APS) switchover occurred on two Cisco 10000 series routers, MLPPP interfaces on the router with the new active APS interface stayed in the Up/Down state. This was observed when two Cisco 10000 series router were configured for MR-APS and were connected using channelized OC-3 line cards or channelized OC-12 line cards. This has been fixed.

Resolved Caveats—Cisco IOS Release 12.0(30)SZ3

This section describes caveats that were fixed in Cisco IOS Release 12.0(30)SZ3.

Cisco IOS Release 12.0(30)SZ3 is based on Cisco IOS Release12.0(30)SZ2 and contains the hardware and software features, and caveats included in Release 12.0(30)SZ2.

CSCed09685

When accounting was enabled using CLI commands, Cisco routers sent the full text of each command to the ACS server. Although the information was encrypted before sending to the server, the server decrypted the packets and logged the commands to the log file in plain text. As a result, sensitive information such as passwords were visible in the server's log files. This occurred only with the accounting enabled commands. This has been fixed.

CSCeg04815

The PXF engine on a Cisco 10000 series router reloaded when the **bump implicit** command was configured on a VC with precedence 1 and the **no bump traffic** command was configured on a VC with precedence 0. This has been fixed.

CSCei16493

When a single-router APS (SR-APS) configuration was removed and then re-applied, the standby PRE2 generated continuous traceback messages. This occurred on a Cisco 10000 series router that was configured with redundant PRE2s functioning in SSO mode and with 4-port channelized STM-1 line cards (part number ESR-4CHSTM1) functioning in linear 1+1 automatic protection system (APS) mode. APS was configured by entering the **associate slot** *slot_one slot_two* command.

CSCek26492

A router sometimes failed if it received a packet with a specific crafted IP option as described in the *Cisco Security Advisory: Crafted IP Option Vulnerability* document, located at the following URL:

http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

This caveat was a symptom of CSCec71950. Only Cisco IOS software that did not include the resolution to CSCec71950 was at risk of failure. This has been fixed.

CSCek38584

When an interface was shut down, the routes that used the down interface as an output interface were deleted by the routing information base (RIB) and then added back by the ISIS protocol, until ISIS finally deleted it after ISIS SPF. As a result, fast convergence was affected. This has been fixed.

CSCek50796

When the proxy vector changed on the router that originated the vector, a PIM join was not triggered, even if the RPF neighbor and the RPF interface remained the same. This occurred in a multicast VPN (MVPN) inter-autonomous system (AS) configuration in which the proxy information was learned from the BGP IPv4 MDT update. This has been fixed.

CSCek54768

E1 interfaces sometimes went down when a line card was reset or removed, even when the line card had automatic protection system (APS) enabled and an APS switchover was triggered. The interfaces came back up within a few seconds. This occurred on a Cisco 10000 series router with a pair of 4-port channelized OC-3 line cards that were configured for single-router APS (SR-APS). The line cards were configured with E1 interfaces under either SONET or SDH.

This symptom occurred only when a line card was reset or removed, not when an APS switchover was triggered by a fiber cable that was removed. The chances of the symptom occurring were reduced when the line card that was reset or removed was not the active line card.

The symptom was due to a change in the E1 clock source that occurred when the line card was reset or removed, and that caused the alarms to be received. The symptom was more likely to occur when the line card had a large configuration and when the E1 interfaces were set to "clock source line." This has been fixed.

CSCek63394

When upgrading from Cisco IOS Release 12.0(25)SX10 to Release 12.0(30)SZ2, a customer observed spurious memory access and a traceback message. This occurred in the customer environment when executing the **show hardware pxf cpu cef** command. This has been fixed.

CSCsa82771

T1 and T3 clocks did not switch to the internal source when LOF-DS3, AIS-DS3, LOF-DS1, or AIS-DS1 alarms occurred. This symptom occurred on a Cisco 10000 series router that was configured with a 1-port channelized OC-12/STM-4 line card or 4-port channelized OC-3/STM-1 line card. This has been fixed.

CSCsb11466

A router acting as DIS did not generate IIH packets to its adjacencies, causing the ISIS adjacencies to flap. Those adjacencies were backed up in a very short period of time (10s of milliseconds). A known trigger for this behavior was bringing down an ISIS adjacency in the upstream router one hop away. This behavior was observed on Cisco 12000 series routers that were running Cisco IOS Release 12.0(25)S4. This has been fixed.

CSCsb50606

Memory usage in the "Dead" process grew gradually until the memory was exhausted. The output of the **show memory dead** command showed that many "TCP CBs" were re-allocated. Analysis of the problem showed that these were TCP descriptors for non-existing active BGP connections. This occurred on a Cisco 7200 series router that was running Cisco IOS Release 12.3(13). The router had an NPE-G1 and functioned as a PE router with many BGP neighbors. However, the symptom was not platform-specific or release-specific. This has been fixed.

CSCsb52717

A Cisco router configured for multicast VPN (mVPN) reloaded after receiving a malformed MDT data group join packet. This affected all Cisco IOS software versions that supported mVPN MDT. This has been fixed.

CSCsb97607

The BIP-2 counters were wrong on the channelized STM-1 line card (part number ESR-CHSTM1). For each 24 hours, the BIP-2 value of the current interval was added to the start values of the 15-minute periods on the channelized STM-1 line card. This occurred on a router running Cisco IOS Release 12.0(27)S5. This has been fixed.

CSCsd12941

CPU usage remained at 99 percent for a long time when the network management system (NMS) polled the ipRouteTable using the SNMP protocol. This occurred on a Cisco router running Cisco IOS Release 12.0(28)S or Release 12.0(31)S and with a large number of routes in the routing table. This symptom might have also occurred when the router was running other Cisco IOS releases. This has been fixed.

CSCse04560

A TFTP client tried to transfer a file from a Cisco IOS device configured as a TFTP server. An access control list applied on the server denied access to the file. However, the TFTP client received a different outcome depending on whether or not the file was offered for download. As a result, a third party might have been allowed to enumerate which files were available for download. This symptom occurred when the following commands were configured on the TFTP server. This has been fixed.

```
Router(config)# tftp-server flash: filename1 access-list-number
!
Router(config)# access-list access-list-number permit 192.168.1.0 0.0.0.255
!
Router(config)# access-list access-list-number deny any
```

CSCse05736

A router that was running RCP was reloaded by a specific packet. This occurred when RCP was enabled on the router. The packet had a specific data content and came from the source address of the designated system configured to send RCP packets to the router. This has been fixed.

CSCse27157

E1 interfaces did not switch to the internal clock when LOF or AIS alarms were detected. This occurred on a Cisco 10000 series router with E1 serial interfaces configured for clock source line on either a channelized OC-3 or channelized OC-12 line card. This has been fixed.

CSCse57324

SONET Link Up and Down event messages for the protection port of an APS pair did not report to the console log. When the fiber was removed from the protection port to simulate a failure on the protection line, a message did not display on the console. This occurred on a Cisco 10000 series router with a single-router APS (SR-APS) configuration on the 4-port channelized OC-3 line card. This symptom might also have affected other line cards on the router that supported SR-APS. This has been fixed.

CSCse95758

You could use an access control list (ACL) to restrict TFTP configuration transfers that were initiated using SNMP by using the **snmp-server tftp-server-list** *access-list* command. For example, the following sample configuration caused the router to reject configuration file transfers using SNMP from all hosts except the TFTP server that was specified in ACL 5. However, implementing this restriction for the FTP, RCP, and SCP protocols was not possible. This occurred on any Cisco IOS router that was configured for SNMP. This has been fixed.

```
snmp-server tftp-server-list 5
!
access-list 5 permit 10.1.1.1
snmp-server community private RW 5
snmp-server tftp-server-list 5
```

CSCsf20111

Traffic intermittently came to a complete halt on a Frame Relay subinterface to which a service policy was applied. This occurred on a Cisco 10000 series router with a PRE1 and running Cisco IOS Release 12.0(25)SX6f. The PXF sometimes stopped dequeuing packets and the interface output queue became stuck. This has been fixed.

CSCsg53742

AU-4-TUG-3 bounced when an interface was shutdown and then brought back up using the **shutdown** and **no shutdown** commands. This occurred on a Cisco 10000 series router running the Cisco IOS 120_28_s3_throttle 050915 image. This has been fixed.

CSCsg54731

Traffic loss was observed on multilink interfaces in a back-to-back configuration. This occurred on a Cisco 10000 series router with a 1-port channelized OC-12 line card and a Multilink PPP configuration. This has been fixed.

CSCsg70355

Starting in calendar year 2007, daylight savings summer-time rules caused Cisco IOS software to generate timestamps that were off by one hour (for example, the timestamp in SYSLOG messages). The Cisco **clock summer-time** *zone* **recurring** command by default used United States standards for daylight savings time rules. The Energy Policy Act of 2005 (H.R.6.ENR), Section 110 changed the start date from the first Sunday of April to the second Sunday of March and changed the end date from the last Sunday of October to the first Sunday of November. This has been fixed.

CSCsg79508

A self-ping operation failed when RPF was configured on the input interface. This occurred on a Cisco 10000 series router running Cisco IOS Release 12.0(28)S3 and Release 12.0(30)SZ. The PXF dropped the self-ping packet because it incorrectly believed that the RPF check had failed. This has been fixed.

CSCsg81770

When the router was configured so that the ifIndex value of 62 was assigned to a subinterface (non-HWIDB), the interface did not show up in the ifMIB output. The only one that seemed to be affected was ifIndex 62. This has been fixed.

CSCsh22146

A DS1 link stalled due to a known hardware issue and stopped passing traffic after a duration. This was fixed by applying a hardware workaround to the bad DS1 link, which enhanced the debugging feature of the chip and allowed specific DS1 links to be targeted for diagnosing the DS1 stall issue. This was done nonintrusively and without risking line card downtime. This has been fixed.

CSCsh62329

Configured serial interfaces did not come up and showed Loss of Pointer errors. This occurred on the Cisco 10000 series router with either a 1-port channelized OC-12 or 4-port channelized OC-3 line card. The line card had E1 or T1 interfaces configured and some ports did not have framing configured on the SONET controller. This has been fixed.

CSCsh71327

Due to an unsupported card, the number of entries in the cardTable of the chassis MIB continued to increase every 5 seconds. This occurred on a router with a PRE1 and an unknown or unsupported card installed in the chassis. This has been fixed.

CSCuk54191

On a Cisco router running Border Gateway Protocol (BGP) and MPLS VPN protocols, a few routes were not installed in a newly created MPLS VPN VRF routing information base (RIB). This occurred when adding and deleting VRFs quickly and continuously, and under rare conditions, and depending on the timing of such operations. When scripts were used to create and destroy VPN VRFs very fast, under some rare conditions this symptom was noticed. This has been fixed.

Resolved Caveats—Cisco IOS Release 12.0(30)SZ2

This section describes caveats that were fixed in Cisco IOS Release 12.0(30)SZ2.

Cisco IOS Release 12.0(30)SZ2 is based on Cisco IOS Release 12.0(30)SZ1 and contains the hardware and software features, and caveats included in Release 12.0(30)SZ1.

CSCdx07308

When two separate HSRP groups were misconfigured with the same standby IP address, an ARP storm occurred and the affected interfaces experienced bad or no connectivity. Warnings displayed on the console such as %IP-4-DUPADDR and %SYS-2-MALLOCFAIL. The exact process that reported the malloc failure was usually either "IP Input," "ARP Input," or "Pool Manager." This problem affected Cisco IOS Release 12.2(5) and later releases. This has been fixed.

CSCea40884

A Cisco router sometimes reloaded when you entered the **show ip route vrf** *vrf-name* command in privileged EXEC mode. This symptom was router and release independent. This has been fixed.

CSCed81202

The following error and traceback messages sometimes displayed after an interface transition. This occurred on the Cisco 10000 series router with MPLS configured. This has been fixed.

```
Feb 20 06:11:02.995 MET: %GENERAL-3-EREVENT: HWTAG:Invalid s/w taginfo.

-Traceback= 600A6700 607B1438 607AF254 607AACE0 607AB0C8 607ADA38 6020262C
60202EF0 60204AD8
60204C60 60204F00 602081F8 602E6EBC 602E6EA8
```

CSCee55828

The 1-port channelized OC-12 line card could not be configured with the **t1 1 framing esf** and **t1 1 loopback remote** commands at the same time. This occurred on a Cisco 10000 series router and the **t1 1 framing esf** command was configured under AU-4 on the line card. This has been fixed.

CSCeg34589

On a Cisco 10000 series router, when you first attached a Frame Relay map class to a channelized T3 subinterface and then attached the input service policy to the main interface, the **set** command in the input policy did not remark the packets. This did not occur when you first attached the input policy to the main interface and then attached the Frame Relay map class to the channelized T3 subinterface. However, when you then removed the input policy, the packets continued to be remarked. This has been fixed.

CSCeh49776

The SNMP mplsOutSegmentTable did not contain entries for the reserved **explicit-null** label. However, these labels were indicated in the output of the **show mpls forwarding** command as the following sample output shows. The two entries with **[V]** did not show up in a MIB walk of mplsOutsegmentTable. This has been fixed.

```
PE-802> show mpls forwarding
  Local  Outgoing      Prefix            Bytes Label   Outgoing   Next Hop
  Label  Label or VC   or Tunnel Id      Switched      interface
  16     Pop Label     10.3.4.0/24       0             Et1/0      10.2.3.3
  17     Pop Label     172.16.3.3/32     0             Et1/0      10.2.3.3
  18     17            172.17.4.4/32     0             Et1/0      10.2.3.3
  19     No Label      172.18.1.1/32[V]  0             Et0/0      10.1.2.1
  20     Aggregate     10.1.2.0/24[V]    0             vpn1
```

CSCei09385

A 4-port channelized OC-3/STM-1 line card reset during an SSO switchover. This occurred on a Cisco 10000 series router when the 4-port channelized OC-3/STM-1 line card was operating fully configured with the maximum number of configurable interfaces (768 T1 or E1 interfaces) at 90 percent of the maximum traffic rate. This has been fixed.

CSCei38386

While running weighted random early detection (WRED) tests, a Barium Failed Enable event occurred and the Cisco IOS software restarted. This occurred with the 7xi-050623 and 7xi_050626 software images. A log error was detected with the following traceback message. This has been fixed.

```
-Traceback= 6054832C 605488C0 60549B1C 6012E85C 60EB5400 600F3F60 6012E8C0 60D0E4AC
60D13588 60D135C4 60DD00FC 603BBF20 60142B10 603D5EBC 604675E4 604675C8
```

CSCek39365

The incorrect inbound interface VCCI was sometimes programmed into the PXF for RP discovery group (224.0.1.40). This resulted in RP mapping information aging out because RP discovery messages were not processed by the PXF. This symptom occurred on a Cisco 10000 series router running Cisco IOS Release 12.0(28)S2 or later releases and the router was configured for multicast VPN (mVPN). The customer VRF used Auto-RP. This has been fixed.

CSCek54251

During BERT testing of the DS3 port with different patterns, the error counters showed zero when errors were introduced. Sometimes the BERT testing error counters incremented even though errors were not introduced. This has been fixed.

CSCsa63383

The ignored and input drop counters on a half-height Gigabit Ethernet interface sometimes increased by 65536 when a CRC or runt error occurred. This was observed on a Cisco 10000 series router running Cisco IOS Release 12.3(7)XI2 and with a half-height Gigabit Ethernet line card on which a few CRC or runt errors occurred. The **show interface** command was used to display the number of ignored errors, input drops, CRCs, input errors and so on. This has been fixed.

CSCsb09807

The SSO switchover time was too long on a channelized OC-3 or OC-12 line card that was configured for PPP, Frame Relay, and HDLC encapsulation. The traffic interruption lasted between three and 40 seconds. This symptom was observed on a Cisco 10000 series router configured with redundant PREs functioning in SSO mode and with one or more 1-port channelized OC-12/STM-4 or 4-port channelized OC-3/STM-1 line cards configured with any type of encapsulation. This has been fixed.

CSCsd15749

Prefixes that were tagged with Site of Origin (SoO) values were sometimes not filtered at the border. This occurred when SoO values were configured for a peer group. The peer group members did not always correctly filter the prefixes that were based on the SoO value at the border. This has been fixed.

CSCsd41586

When issuing a **show running-config** command, a system sometimes experienced a failure due to a bus error. This occurred on a Cisco 10000 series router when the **show startup-config** command was still executing in another terminal window and the output was not finished displaying. Other concurrent operations that accessed the NVRAM could have led to similar problems and other systems could have experienced this issue. This has been fixed.

CSCsd64204

A router failed or reported spurious memory access when the **show ip bgp neighbor** *x.x.x.x policy* command was issued for a configured peer. This has been fixed.

CSCsd65958

When the Layer 2 traffic contained broadcast traffic, the number of packets per second was far greater than the number of bytes per second on some of the line card interfaces, which is impossible. This has been fixed.

CSCse30032

Some ping operations failed when pinging an interface (belonging to a VRF on a router) across a MPLS VPN backbone. Tag packets destined for the local router became corrupted in the PXF if the trunk interface had a service policy that manipulated IP precedence or DSCP settings. This occurred on a Cisco 10000 series router with a PRE1 and was observed when the router was running Cisco IOS Release 12.0(27)S and Release 12.0(30)S. This has been fixed.

CSCse58444

When changing channel group configurations on a Cisco 10000 series router, the line cards sometimes reset. This occurred with a 1-port channelized OC-12 line card and a 4-port channelized OC-3 line card. The reset was rare, but was seen when traffic was flowing on channelized interfaces and the channel group configuration on a T1 or E1 was changed without first removing the existing channel groups. This has been fixed.

CSCse71145

A potential problem existed with the EHSA component of the software, specifically the code that used ehsa_standby_comm_prep(). This problem might have caused the software to fail. In rare instances, this problem occurred when using the **banner** command, but was not otherwise reproducible. This has been fixed.

CSCse83061

The changes implemented for CSCse58444 and CSCse74622 caused the 1-port channelized OC-12 and 4-port channelized OC-3 line cards to reset unexpectedly. This occurred on the Cisco 10000 series router when changing configurations while traffic was flowing. This has been fixed.

CSCse83989

When you reset or inserted a line card while traffic was flowing, the line card sometimes reset continuously. This occurred on a Cisco 10000 series router with a 1-port channelized OC-12 line card and a 4-port channelized OC-3 line card. This has been fixed.

CSCse88094

The Cisco 7200 router failed when executing alias commands. Certain conditions led to the failure, such as when a session (console or VTY) tried to display aliases using the **show aliases** command and at the same time another session (SNMP) removed or changed some of the aliases. This is because the printf() function of the **show aliases** command accessed the already freed memory location. This has been fixed.

Resolved Caveats—Cisco IOS Release 12.0(30)SZ1

This section describes caveats that were fixed in Cisco IOS Release 12.0(30)SZ1.

Cisco IOS Release 12.0(30)SZ1 is based on Cisco IOS Release12.0(30)SZ and contains the hardware and software features, and caveats included in Release 12.0(30)SZ.

CSCeg11566

Intensive SNMP polling sometimes caused the I/O memory of a router to be depleted. This was observed in rare situations. This has been fixed.

CSCej56341

T1 controllers in AIS that responded to a remote loop command did not resume sending AIS when the loop was removed. Because the router terminates a T1 chain, the only time it transmits AIS is when it is administratively down. For the 6-port channelized T3 line card, this problem occurred when no channel groups were assigned to the T1 (for example, the T1 controller had no explicit **shutdown** command and was accessed using the channelized T3 controller commands). This has been fixed.

CSCsa62939

When the **show aps controller** command was issued in user mode or privileged EXEC mode, the PRE2 configured with automatic protection system (APS) sometimes reloaded with a bus error exception. This occurred on a router running Cisco IOS Release 12.3(7)XI2. This has been fixed.

CSCsc12244

Packets were dropped on a multilink PPP (MLPPP) link for certain applications. This has been fixed.

CSCsc28439

When performing a redundancy switchover or during system startup, the following error messages sometimes appeared. This occurred on the Cisco 10008 router. This has been fixed.

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x605ECA04 reading 0x8
%ALIGN-3-TRACE: -Traceback= 605ECA04 605E611C 6042DCCC 6042DD4C 603C7ED8 603A5F84 603A6458
601A67E8
```

CSCsc78957

After a switchover, the PoS interface's link protocol did not come up on the Cisco 10008 router and the following error message appeared. This has been fixed.

```
"PXF_DMA-3-IRONBUS_NOTRUNNING"
```

CSCsd33244

Packet forwarding stopped on the Fast Ethernet line card of a Cisco 10000 series router running Cisco IOS Release 12.0 S. The length of output queues on all line card interfaces constantly increased. The line protocol on the interfaces remained Link Up, Protocol Up. This problem was observed using the **show hardware pxf cpu queue FastEthernet4/1/3** command in privileged EXEC mode. This has been fixed.

CSCsd38657

A route processor (RP) failed when a Gigabit Ethernet interface of a SPA was shut down. The following error and traceback messages were generated:

```
Unexpected exception to CPUvector 700, PC = 2CEE34
-Traceback= 2CEE34 4C40000 2D8958 2D8D2C 2C1164 14048C 2CFB4C
```

If a crashinfo file was generated, the last log message was the following:

```
%SYS-6-STACKLOW: Stack for process CEF process running low, 0/6000
```

On a router that was configured with two RPs functioning in RPR+ mode, when the RP failed, a switchover occurred. However, the failed RP did not come up and remained in standby mode.

These symptoms were observed on a Cisco router when the recursive lookup on a static MPLS route did not specify a next hop interface. For example, the symptom occurred when the **ip route** *destination-prefix mask next-hop1* command was enabled, but did not occur when the **ip route** *destination-prefix mask interface1 next-hop1* command was enabled.

CSCsd43617

On the Cisco 10000 series router, an interface on the 8-port Fast Ethernet line card could negotiate down to half-duplex mode. This occurred when the Cisco 10000 series router was connected to a Cisco 3600 router and full duplex was configured on the Fast Ethernet ports of both routers. This has been fixed.

CSCsd53814

A Cisco 10008 router with a 6-port channelized T3 line card sometimes experienced a %IPCOIR dump and all ports on the line card reset. This was observed on a Cisco 10008 router running Cisco IOS Release 12.0(27)S2. This has been fixed.

CSCsd62472

A Cisco 10000 series router running Cisco IOS Release 12.0(26)S5 experienced alignment errors while forwarding traffic. This has been fixed.

CSCsd86134

The PXF engine punted multilink PPP (MLPPP) packets to the route processor (RP). This occurred when the MLPPP packets' inner PPP header had a compressed protocol field. This has been fixed.

Resolved Caveats—Cisco IOS Release 12.0(30)SZ

This section describes caveats that were fixed in Cisco IOS Release 12.0(30)SZ.

Cisco IOS Release 12.0(30)SZ is based on Cisco IOS Release 12.0(30)S5 and contains the hardware and software features, and caveats included in Release 12.0(30)S5.

CSCsc52732

When PIM was enabled or disabled on a subinterface, multicast traffic that was received on another subinterface of the same main interface was dropped for a moment. This occurred on a Cisco router that was configured for IP Multicast. The higher the multicast traffic rate, the more packets were dropped. This has been fixed.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html