Caveats for Cisco IOS Release 12.2(33)SRA through 12.2(33)SRA7

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 this section.

Because Cisco IOS Release 12.2SR is based on Cisco IOS Release 12.2, many caveats that apply to Cisco IOS Release 12.2 also apply to Cisco IOS Release 12.2SR. For information on severity 1 and 2 caveats in Cisco IOS Release 12.2, see the *Caveats for Cisco IOS Release 12.2* document located on Cisco.com.

In this section, 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.

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 **Support: Tools & Resources: Bug Toolkit** (which is listed under Troubleshooting). Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may 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.)

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

Resolved Caveats—Cisco IOS Release 12.2(33)SRA7

Cisco IOS Release 12.2(33)SRA7 is a rebuild release for Cisco IOS Release 12.2(33)SRA. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRA7 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCeb69473

  Symptoms: Device crashes with a segmentation violation (SegV) exception.

  Conditions: Occurs when the **connect** *target_ip* **[login|513] /terminal- type** *value* command is entered with a large input parameter to the *terminal-type* argument such as the following:

```
router>connect 192.168.0.1 login /terminal-type aaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Trying 192.168.0.1...Open
login:


*** System received a SegV exception ***
signal= 0xb, code= 0x1100, context= 0x82f9e688
PC = 0x61616160, Vector = 0x1100, SP = 0x833ae5a8
```

  Workaround: AAA Authorization AAA authorization enables you to limit the services available to a user. When AAA authorization is enabled, the network access server uses information retrieved from the user's profile, which is located either in the local user database or on the security server, to configure the user's session. Once this is done, the user will be granted access to a requested service only if the information in the user profile allows it.

  For a complete description of authorization commands, refer to the following links:

  ACS 4.1 Command Authorization Sets

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/SPC.html

  ACS 4.1 Configuring a Shell Command Authorization Set for a User Group

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/GrpMgt.html

  Role-Based CLI Access The Role-Based CLI Access feature allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (Config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco networking devices. The following link provides more information about the Role-Based CLI Access feature:

  Role-Based CLI Access

  http://www.cisco.com/en/US/docs/ios/12_3t/12_3t7/feature/guide/gtclivws.html

Device Access Control Due to the nature of this vulnerability, networking best practices such as access control lists (ACLs) and Control Plane Policing (CoPP) that restrict vulnerable device access to certain IP addresses or Subnetworks may not be effective. Device access best practices provide some mitigation for these issues by allowing systemic control of authenticated and unauthenticated users. Device access best practices are documented in:

Infrastructure Protection on Cisco IOS Software-Based Platforms Appendix B-Controlling Device Access:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6970/ps1838/prod_white_paper0900aecd804ac831.pdf

Improving Security on Cisco Routers http://www.cisco.com/warp/public/707/21.html

- CSCee89849

  Symptoms: A router may reload due to an illegal access at a low address.

  Conditions: This symptom is observed on a Cisco router when AAA is enabled.

  Workaround: There is no workaround.

- CSCeg25475

  Symptoms: Filtering BGP routes by means of the **distribute-list prefix MARTIAN in** command applied to address-family IPv4, actually filters out M-BGP routes in address-family vpnv4.

  Conditions: This symptom occurs when MPLS-VPNs are configured.

  Workaround: Use route-maps to filter routes inbound.

  Further Problem Description: It can be checked by means of the **show ip bgp neighbors** command that the prefixes are actually being filtered out from updates for address-family VPNv4, and not for IPv4, as it is configured.

- CSCek54959

  Symptoms: During switchover following error message appears:

  ```
  %MFI-3-REDISTMGR: Redistribution Manager: register - null LSD 16.
  ```

  Conditions: There is no specific condition. A switchover is done with MPLS application enabled.

  Workaround: There is no workaround.

- CSCek78675

  Symptoms: SIP200 may crash multiple times on executing the QoS test cases.

  Conditions: This symptom occurs while configuring/unconfiguring different QoS features and running traffic for a while.

  Workaround: There is no workaround.

- CSCin99430

  Symptoms: Running the **snmpwalk** command on ifInOctets and some other ifMIB objects is not returning values for all the interfaces. The **snmpget** command is working fine.

  Conditions: This symptom occurs when the hidden command **no snmp- server sparse-table** is configured.

  Workaround: Configure hidden command **snmp-server sparse- table**.

- CSCsd47475

  Symptoms: A Cisco Catalyst 6000 series switch or Cisco 7600 series router may not be able to resolve ARP requests.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with an enhanced FlexWAN module (WS-X6582-2PA) in which a 100BASE-TX port adapter (PA-FE-TX) and an IPSec VPN Acceleration Services Module (WS-SVC-IPSEC-1) are installed.

Workaround: Configure a static ARP entry.

- CSCse44079

  Symptoms: The CPU usage may reach 100 percent in the IGMP Input process when a ULD interface is down.When the downstream UDL interface (on downstream router) down, any (downstream router) local received IGMP report/leave will be sent to router itself 255 times and cause the high CPU.

  Conditions: This symptom is observed on a Cisco router that has a UDL interface that is connected to a satellite link after you have upgraded the Cisco IOS software image from Release 12.4(5a) to Release 12.4(7a). However, the symptom is not release-specific.

  Workaround: There is no workaround.

  Further Problem Description: When the UDL link goes down, the downstream router starts to flood IGMP reports to himself, and in the Cisco IOS Releases 12.4(7a), 12.4(8), 12.3(19) theCisco IOS is really processing this packets, which has a big impact on the CPU utilization.

- CSCsg39295

  Symptoms: Password information may be displayed in a Syslog message as follows:

  ```
  %SYS-5-CONFIG_I: Configured from scp://userid:password@10.1.1.1/config.txt by
  console
  ```

  Conditions: When using SNMP to modify a configuration by means of the CISCO-CONFIG-COPY-MIB, selection of ConfigCopyProtocol of SCP or FTP may result in the password being exposed in a syslog message.

  Workaround: When using SNMP to modify a configuration by means of the CISCO-CONFIG-COPY-MIB, use the ConfigCopyProtocol of RCP to avoid exposure of the password.

- CSCsg40573

  Symptoms: A Cisco 7600 series may enter a state in which the FIB is frozen, and the syslog may show information similar to the following:

  ```
  %MLSCEF-SP-2-SANITY_FAIL: Sanity Check of MLS FIB s/w structures failed
  %MLSCEF-SP-2-FREEZE: hardware switching disabled on card
  ```

  In this frozen state the data plane is not affected, but new forwarding information does not take effect on the hardware, causing an inconsistency between MPLS or IP software forwarding and the hardware.

  Conditions: This symptom is observed when the TCAM information for a label or prefix and mask does not match the software version, which prevents the TCAM driver from deleting the label or prefix and mask. For example, the symptom may occur when a label is moved from one type (for example, form an aggregate label) to another other type (for example, to a non-aggregate label).

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the router.

  Further Problem Description: You can check the status of the FIB by entering the **show mls cef hardware | i TCAM** command. When the symptom has occurred, the output of this command shows the following:

  ```
  CEF TCAM v3: (FROZEN)
  ```

- CSCsi26184

  Symptoms: A router may crash and generate the following error messages:

  ```
  %SYS-2-CHUNKBOUNDSIB: Error noticed in the sibling of the chunk pak subblock
   -Process= "LFDp Input Proc"
   %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk
   -Process= "LFDp Input Proc"
   %Software-forced reload
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB2 and that is configured for MPLS. Note that the symptom is not release-specific.

  Workaround: There is no workaround. Note that the symptom does not occur inCisco IOS Release 12.2(28)SB5.

- CSCsj73669

  Symptoms: Link flaps may intermittently occur on TenGigabit Ethernet interfaces with certain Xenpak transceivers.

  Conditions: This problem only occurs on 10GBASE-SR. As DOM is not supported for this Xenpak type by Cisco IOS, the interaction between the Xenpak DOM hardware and the Cisco IOS DOM polling mechanism may cause the link to flap.

  Workaround: There is no workaround.

- CSCsj83102

  Symptoms: RP may crash with a bus error while trying to configure card type on a PA in a Flexwan while that PA/Flexwan is experiencing communication problems with the SUP.

  Conditions: This is a rare issue which is only seen under certain circumstances when a configuration is attempted on a card which is itself experiencing communication problems with the rest of the chassis/reloading, crashing, and other problems.

  Workaround: Avoid issuing the **card type** command while the PA/Flexwan is experiencing problems. If the card in question is experiencing hardware issues, the problem may also be avoided by replacing the card.

- CSCsj85065

  A Cisco IOS device may crash while processing an SSL packet. This can happen during the termination of an SSL-based session. The offending packet is not malformed and is normally received as part of the packet exchange.

  Cisco has released free software updates that address this vulnerability.

  Aside from disabling affected services, there are no available workarounds to mitigate an exploit of this vulnerability.

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

- CSCsj88208

  Symptoms: The digital optical monitoring (DOM) feature may be disabled on Xenpak modules of the type SR, LR, ER, LR+, and ER+. However, when this situation occurs, the Xenpak modules can still be used to pass traffic.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that runs Cisco IOS Release 12.2(33)SXH or Release 12.2(33)SRB.

  Workaround: There is no workaround.

Further Problem Description: Note that an LR+ Xenpak module is an LR Xenpak module with a part number of "10-1838-04" and that an ER+ Xenpak module is ER Xenpak module with a part number of "10-1888-04".

- CSCsk06769

  Symptoms: Shut of any LAN interface can cause the MAC address table to go bad, and all the traffic flowing through that VLAN may stop.

  Conditions: The **show mac-address-table dynamic** command shows that all the MAC addresses are learned on the BCP trunk port which is WAN link.

  Workaround:

  1. Though not valid but **shut/no shut** of the WAN link can re-establish the MAC address table correctly.
  2. Use static MAC address entries for all MAC addresses to be learned over WAN interface using the **mac-address-table static** *mac- add* **vlan** *id* **interface** *id* command. Make these static entries on both ends.

- CSCsk07255

  Symptoms: A Sip-600 may reload when an SSO switchover is performed.

  Conditions: The problem is observed in a Cisco 7600 series router with redundant supervisor engines and a SIP-600 line card. The SIP-600 may reload when an SSO switchover is performed between the Active and Standby supervisor engines.

  Workaround: There is no workaround.

- CSCsk32209

  Symptoms: Crash is seen in generating RSA keys.

  Conditions: This symptom happens before applying **crypto map** command.

  Workaround: There is no workaround.

  Further Problem Description: This problem is not seen on SUP730 or SUP32. It is only seen on RSP720. It is due to local variables that are used globally.

- CSCsk33740

  Symptoms: Increasing the IPSec anti-replay window size to 1024 by the **crypto ipsec security-association replay window-size** [*1024*] command could cause the following error messages:

  ```
  Aug 17 11:10:33 PDT%SPA-IPSEC-2G-4-ICPUPP13: slot 4/2 Policy check failed for
  pkt src:192.168.2.2 dst:172.16.2.84 proto:17 SA index:0x9307
  ```

  and/or

  ```
  Jul 28 23:53:16.276%SPA-IPSEC-2G-4-ICPUPP9: slot 9/2 Packet src:172.21.26.43
  dst:10.1.69.209.109 seq num:0x6cc failed replay check last seq num:0x803fffff
  for SA:0xc6a4.
  ```

  Workaround: Remove **crypto ipsec security-association replay window- size** [*1024*].

- CSCsk41134

  Symptoms: Several problems can be observed when using VPNs on routers related to the parsing of the ID payload of the client. Possible symptoms include:

  – the RSA signature negotiation fails with a "signature invalid" message.

  – the certificate based authentication with ISAKMP profiles will not select the correct profile, and the connection will use the default settings.

In all these cases the ISAKMP negotiations do not work.

Conditions: This symptom occurs when using certificate based authentication with ISAKMP profiles.

Workaround: There is no workaround.

Further Problem Description: After enabling ISAKMP debugging you will see in the first case:

```
ISAKMP:(68001): processing SIG payload. message ID = 0
 ISAKMP:(68001): signature invalid!
```

or possibly

```
ISAKMP (0:13005): FSM action returned error: 2
```

In the second case you will either see:

```
ISAKMP:(68001): processing ID payload. message ID = 0
 ISAKMP (68001): ID payload
 next-payload : 6
 type         : 9
 Dist. name parsing failed
 protocol     : 17
 port         : 500
 length       : 185
 ISAKMP:(68001):: UNITY's identity FQDN but no group info
 ISAKMP:(68001):: peer matches *none* of the profiles
```

Or

```
00:03:18: ISAKMP (0:268435457): ID payload
 next-payload : 6
 type         : 9
 Dist. name   :
 protocol     : 17
         port         : 500
 length       : 73
```

(Notice the empty "Dist. name" field)

- CSCsk47954

  Symptoms: The **show running-config** command takes 30 seconds to display the configurations.

  Conditions: The “module provision 1 first-insert” configuration was present when this issue was seen. This problem is seen in VTY line, whereas the **show running-config** command executed from the CONSOLE line displays the configurations without any delay. This symptom is seen in rare situations.

  Workaround: If the **show running-config** command output needs to be displayed without 30 seconds delay, the CONSOLE line can be used to run this command.

- CSCsk60769

  Symptoms: K1K2 values are not reflected correctly when the Tx cable on the protect channel on Cisco 7600 POS interface is pulled out or when there is any LRDI alarm.

  Conditions: This symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRB.

Workaround: There is no workaround.

- CSCsk61790

  Symptoms: Syslog displays password when copying the configuration via FTP.

  Conditions: This symptom occurs when copying via FTP. The Syslog message displays the password given by the user as part of syntax of FTP copy.

  Workaround: There is no workaround.

- CSCsk63233

  Symptoms: When SPA on one slot is shut, the other one takes over. If the Cheronia is reset after this, the router crashes.

  Conditions: This symptom is seen under the following conditions:

  1. Two zambonis with redundancy are configured.
  2. The Active SPA should be shut down.
  3. Reset on Cheronia after the standby takes over.

  Workaround: There is no workaround.

  Further Problem Description: Have two zambonis with redundancy configured between them. There are 500 vti tunnels, 500 IVRF and 1 FVRF configured. On shutting down the SPA in 1/1 slot, 1/0 takes over, and then on resetting the Cheronia, the router crashes.

  The crash can be seen with just 1 tunnel, 1 IVRF and a FVRF.

  Steps to reproduce:

  1. Configure the router with the attached configurations
  2. Shut down the spa in slot 1/1.
  3. Once the spa in slot 1/0 takes over, reset the Cheronia in slot 1. 4. The router Crashes.

- CSCsk67457

  Symptoms: Traffic stops flowing on an interface that is configured for Bridge Control Protocol (BCP) over Multilink PPP (MLP).

  Conditions: This symptom is observed on a cisco 7600 series when one of the member links of the MLP interface is shut down.

  Workaround: Bring up the member link that is shut down.

  Alternate Workaround: Reset the MLP bundle interface.

- CSCsk78390

  Symptoms: A crash is seen when we do FPD upgrade paralleL.

  Conditions: This symptom is observed when there is a parallel FPD upgrade.

  Workaround: Do a single FPD upgrade at a time.

- CSCsk86114

  Symptoms: Sometimes, a 7600-SIP-200/7600-SIP-400 on a Cisco 7600 series router reports memory corruption and restarts.

  Conditions: This happens when LFI is enabled on multiple ATM VCs of an ATM interface on an ATM-SPA hosted by 7600-SIP-200/7600-SIP-400.

  Workaround: There is no workaround.

- CSCsk86642

  Symptoms: SPA-2xOC3-POS is not seeing the correct K1/K2 bytes on working group 1 APS, when switching from Protect to Working port.

  Conditions: This was observed in a lab environment with a Cisco 7604 router back to back with a Cisco 7206 router. Code tested Cisco IOS Release SRA1 and Cisco IOS Release SRA2.

  Workaround:

  1. Hw-slot reset on the Sip400-SPA corrects the problem.
  2. A **shut/no shut** on the protect interface corrects the problem.

- CSCsl24391

  Symptoms: A Cisco 7600/SUP-720/WS-6582-2PA/PA-A6-OC3 that is running Cisco IOS Release 12.2(33)SRA2 configured for ATM local switching may experience a condition where the Local Switching cross connect fails to pass traffic. This will be accompanied by **show atm pvc** reporting:

  ```
  Remote Circuit Status = F1 Alarm, Alarm Type = LOS
  ```

  Conditions: This symptom occurs when ATM local switching is configured. This issue occurs when both SONET ATM interfaces enter a S-LOS state at or near the same time, which may result in traffic loss.

  Workaround: Removing and re-adding the **connect** command alleviates the condition.

- CSCsl41230

  Symptoms: VPN SPA, with crypto map interesting traffic based on TCP ports, is broken.

  ```
  ip access-list extended b2b-pokus
   permit tcp host 10.150.20.13 eq telnet 10.13.11.0 0.0.0.255
   permit tcp host 10.150.20.11 eq telnet 10.13.11.0 0.0.0.255
   permit tcp host 10.13.0.1 10.13.11.0 0.0.0.255 eq telnet
   permit tcp host 10.13.0.2 10.13.11.0 0.0.0.255 eq telnet
   permit tcp host 10.13.0.3 10.13.11.0 0.0.0.255 eq telnet
  ```

  Conditions: This symptom is observed on s72033-advipservicesk9_wan-mz.122- 33.SXH.bin.

  Workaround: The problem is not seen with s72033-advipservicesk9_wan-mz.122- 18.SXF7.bin.

  Further Problem Description: This also fails for deny statements based on TCP ports in the crypto ACL. The SPA will encrypt this traffic that should be denied.

- CSCsl54243

  Symptoms: A SIP-400 will crash on a Cisco 7600 series router after inserting an SPA then removing a VLAN subinterface.

  Conditions: This symptom is observed on a Cisco 7600 series router with a SIP- 400 line card running Cisco IOS Release 12.2(33)SRA5. VLAN subinterfaces that exist prior to inserting an SPA will cause the SIP to crash if they are unconfigured after inserting another SPA.

  The specific steps that cause the SIP-400 to crash are:

  1. Configure a VLAN subinterface on an SPA. 7600(config)#int gi 2/0/0.100 7600(config-subif)#encap dot1q 100
  2. Physically insert another SPA into the SIP-400.
  3. Unconfigure the subinterface and observe the SIP-400 crash. 7600(config)#no int gi 2/0/0.100

  Workaround: There is no workaround.

- CSCsm12247

  Symptoms: A Cisco IOS router configured for WCCP may stop redirecting traffic following a change in topology.

  Conditions: The router must be configured for WCCP redirection using the hash assignment method. When there is only a single appliance in the service group, the loss of hash assignment details is permanent. However with multiple appliances in the group, the loss of assignment information is transitory; the router soon recovers.

  Workaround: To recover the assignment details, the WCCP configuration needs to be removed and re-added to the router. Use the **no ip wccp** *service* command followed by **ip wccp** *service args* command.

Resolved Caveats—Cisco IOS Release 12.2(33)SRA6

Cisco IOS Release 12.2(33)SRA6 is a rebuild release for Cisco IOS Release 12.2(33)SRA. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRA6 but may be open in previous Cisco IOS releases.

Interfaces and Bridging

- CSCek65222

  Symptoms: A non-parseable Ethernet configuration is nvgened for a VLAN.

  Conditions: This symptom is observed when you enter the **encap dot1q 1 native** command, and the command is rejected. When you enter the **encap dot1q 1** command, the command is accepted. However, in this situation, the output of the **show running-config** command shows that the **encap dot1q 1 native** command is present, which would have been rejected.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCse99493

  Symptoms: A router that is configured for NAT Overload may crash while performing dynamic translation from many ports to one port.

  Conditions: This symptom is observed after more than 5000 translations have been performed.

  Workaround: There is no workaround.

- CSCsg55591

  Symptoms: When there are link flaps in the network, various PE routers receive the following error message:

  ```
  %BGP-3-INVALID_MPLS: Invalid MPLS label (1) received in update for prefix
  155:14344:10.150.3.22/32 from 10.2.2.1
  ```

  Or, a local label is not programmed into the forwarding table for a sourced BGP VPNv4 network.

  Conditions: These symptoms are observed when an iBGP path for a VPNv4 BGP network is present, and then a sourced path for the same route distinguisher (RD) and prefix is brought up.

  Workaround: Remove the iBGP path. Note that when the sourced path comes up first, the symptoms do not occur.

Alternate Workaround: Use different RDs with the different PE routers. When the RD and prefix do not match exactly between the iBGP path and the sourced path, the symptoms do not occur.

- CSCsg97662

  Symptoms: When you enter the **no ip nat service skinny tcp port 2000** command, NAT is not disabled on port 2000. This situation causes NAT to be applied to SCCP packets, and causes the CPU usage to be very high.

  Conditions: This symptom is observed when an application is running on the port 2000.

  Workaround: There is no workaround.

  Further Problem Description: SCCP and NAT for voice are not supported in Cisco IOS Release 12.2 or a release that is based on Release 12.2. The **no ip nat service skinny tcp port 2000** command is not supported in these releases.

ISO CLNS

- CSCsj72039

  Symptoms: The prefix of a serial interface that is configured for PPP or HDLC and that functions as a passive interface for IS-IS may not be installed in the local IS-IS database.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18)SXF6 but is not release-specific.

  Workaround: Remove and reconfigure the **passive-interface** command.

  First Alternate Workaround: Enter the **clear isis *** command.

  Second Alternate Workaround: Enter any command that triggers the generation of the local IS-IS database.

Miscellaneous

- CSCdz55178

  Symptoms: A router that is configured for QoS may reload unexpectedly or other serious symptoms such as memory corruption may occur.

  Conditions: This symptom is observed on a Cisco router that has a cable QoS profile with a name that has a length that is greater than 32 characters as in the following example:

```
cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C
                         00000000011111111111222222222333^
                         12345678901234567890123456789012|
                                                          |
                                                   PROBLEM
                                                  (Variable Overflowed).
```

  Workaround: Change the name of the cable QoS profile qos profile to a length that is less than 32 characters.

- CSCeb35205

  Symptoms: A Cisco router may reload when a subdirectory is created on an Advanced Technology Attachment (ATA) Flash disk.

  Conditions: This symptom is observed when the ATA Flash disk space that is allocated to the subdirectory contains data from previously deleted files.

When a subdirectory is created or extended, it is given space on the ATA Flash disk. If this space contains zeros, the symptom does not occur. However, if the space was previously used, the space does contain data bytes from the previous file, and these data bytes may confuse the file system. This situation may cause the router to reload.

Workaround: Do not create subdirectories on the ATA Flash disk.

- CSCek66590

  Symptoms: A router may crash when you enter the **show hw-module subslot** *slot/subslot* command.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with a SPA services carrier (7600-SSC-400).

  Workaround: There is no workaround.

- CSCek68108

  Symptoms: A "INTSCHED: suspend" error message may be generated on a router that is configured with a SPA-IPSEC-2G, and the router may crash.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch an Cisco 7600 series router after you have removed the crypto map in crypto-connect mode.

  Workaround: There is no workaround.

- CSCsa96972

  Symptoms: A Dbus header error interrupt may occur during a recovery procedure on a DFC3, and the following error message is generated:

  ```
  %EARL_L3_ASIC-DFC5-3-INTR_WARN: EARL L3 ASIC: Non-fatal interrupt Packet
  Parser block interrupt
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when a recovery procedure occurs because of a transient problem in hardware forwarding.

  Workaround: There is no workaround. However, the error message indicates a harmless (non-fatal) error and does not have any impact on the traffic and proper functioning of the platform.

- CSCsb21941

  Symptoms: A supervisor engine may reset unexpectedly, and the following error messages may be generated:

  ```
  %PFREDUN-SP-7-KPA_WARN: RF KPA messages have not been heard for XXX seconds
  %OIR-SP-3-PWRCYCLE: Card in module 1, is being power-cycled (RF request)
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when "super jumbo" frames (greater than 10,000 bytes) are being used.

  Workaround: There is no workaround. The symptom can be mitigated by ensuring that all NICs on the domain are configured with a frame size that is smaller than 10,000 bytes.

- CSCsb74409

  Symptoms: A router may keep the vty lines busy after finishing a Telnet/Secure Shell (SSH) session from a client. When all vty lines are busy, no more Telnet/SSH sessions to the router are possible.

  Conditions: This symptom is observed on a Cisco router that is configured to allow SSH sessions to other devices.

  Workaround: Clear the SSH sessions that were initiated from the router to other devices.

- CSCsd70321

  Symptoms: Traffic stops flowing when you reset a line card and immediately afterwards an SSO switchover occurs.

Conditions: This symptom is observed on a Cisco 7600 series.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the line card.

- CSCsd85278

  Symptoms: A diagnostics test for bus connectivity on a SIP-400 fails.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when the **vlan internal allocation policy ascending** command is enabled.

  Workaround: Remove the **vlan internal allocation policy ascending** command.

- CSCsf11353

  Symptoms: A FlexWAN, FlexWAN2, or SIP-200 may crash when you attach or remove service policies to or from virtual interfaces such as MLP or virtual-template interfaces or when these virtual interfaces flap.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsg09423

  Symptoms: When IPsec SAs flap, traffic loss may occur during the IPsec and IKE rekey.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA when there is a large number of IKE and IPsec SAs (that is, more than 2000 IKE SAs and 4000 IPsec SAs) and when RSA signature authentication is configured.

  Workaround: Reduce the number of IKE and IPsec SAs.

- CSCsg18080

  Symptoms: A router that functions as a responder in an SNMP configuration may crash.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with a SPA-IPSEC-2G after SNMP counters are retrieved for inbound traffic.

  Workaround: Do not use SNMP to obtain counters.

- CSCsg55315

  Symptoms: Packets may be duplicated or triplicated on interface “gig1/1” of a Supervisor Engine 2, Supervisor Engine 32, or Supervisor Engine 720.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with WAN line cards such as an Enhanced FlexWAN, SIP-200, SIP-400, or SIP-600 when SPAN is enabled and when interface “gig1/1” is used to connect to another platform.

  Workaround: Do not use interface “gig1/1” to connect to another platform. Rather, use another interface.

- CSCsg64327

  Symptoms: Tunnels may go down when continuous multicast traffic is processed in VRF mode.

  Conditions: This symptom is observed on a Cisco 6500 series switch and Cisco 7600 series router when the following conditions are present:

  – The initiator is configured in VRF mode and the responder is configured in crypto connect mode.

- OSPF is configured for base connectivity and EIGRP is configured on the GRE tunnel.
- There are four tunnels configured between the hub and spoke.
- Multicast traffic is sent through all tunnels via the **ip igmp static-group** command.

Initially, all tunnels are up and the traffic goes through fine as long as the traffic is not continuously. However, when traffic is sent continuously, all tunnels except for one go down one after another.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, you must reload both the hub and the spoke. Note that clearing the (multicast and unicast) routes by shutting down and bringing up the tunnel interfaces on both sides, and clearing and re-establishing the crypto sessions does not resolve the symptom.

- CSCsg92950

  Symptoms: A software-forced reload may occur on a Cisco 7301.

  Conditions: This symptom is observed on a Cisco 7301 that terminates several thousand broadband subscribers. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCsh46565

  Symptoms: When the configuration of the shape average is changed, the rate is not applied, which can be shown in the output of the **show policy interface** command and detected by a traffic analyzer.

  Conditions: This symptom is observed on a Cisco 7600 series that has a Supervisor Engine 720 and GE-WAN subinterfaces that are configured with an HQoS (LLQ) output policy when the shape average is changed on all GE-WAN subinterfaces at the same time.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, delete the output policy and then reconfigure it on the GE-WAN subinterfaces.

- CSCsh61002

  Symptoms: When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a port-based EoMPLS interface (when Xconnect is configured on the main interface), forwarding stops on another L3 interface.

  Conditions: This symptom is observed on a Cisco 7600 series only when there is a short interval (about 30 seconds) between the **shutdown** and **no shutdown** commands.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the router.

  Further Problem Description: When you enter the **shutdown** command quickly followed by the **no shutdown** command on the port-based EoMPLS interface, a new internal VLAN is used. However, because of a software issue, an EoMPLS flag is set on the old VLAN, causing the router to process all packets that are received on the old VLAN as L2 packets. When a new L3 interface comes up and uses the old VLAN, the datapath fails because the router attempts to process these packets as L2 packets instead of L3 packet.

- CSCsi42769

  Symptoms: Tunnels are not set up or data traffic does not go through on a router that uses a VPN SPA card (SPA-IPSEC-2G).

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that uses a SPA-IPSEC-2G with certificates.

  Workaround: There is no workaround.

- CSCsi56793

  Symptoms: The following error messages and tracebacks may be generated on the console of a WAN line card that is installed in a Distributed Forwarding Cards (DFC):

  ```
  DFC1: PXF clients started, forwarding code operationalUnexpected call:
  c6k_pwr_get_system_power_sufficiency()

  DFC1: -Traceback= 4057162C 40B4770C 40B454A0 401EF56C 401EF5FC 4011760C
  40117838 401F089C 401F0888Unexpected call: sp_power_mgmt_led()

  DFC1: -Traceback= 40571F08 40B4771C 40B454A0 401EF56C 401EF5FC 4011760C
  40117838 401F089C 401F0888Unexpected call: sp_module_led()

  DFC1: -Traceback= 40571F30 40B47808 40B454A0 401EF56C 401EF5FC 4011760C
  40117838 401F089C 401F0888Unexpected call: sp_system_led()

  DFC1: -Traceback= 40571F84 40B4783C 40B454A0 401EF56C 401EF5FC 4011760C
  40117838 401F089C 401F0888
  ```

  Conditions: This symptom is observed on a Cisco 7600 series when the WAN line card boots.

  Workaround: There is no workaround. However, the error messages and tracebacks are harmless and do not impact the functionality of the router.

- CSCsi59267

  Symptoms: After you have reloaded the router, the Control Plane Policing feature does not function.

  Conditions: This symptom is observed on a Cisco 7600 series that has a policy attached to the control plane.

  Workaround: Remove the policy from the control plane and then re-attach it.

  Further Problem Description: When the symptom occurs, the output of the **show mls qos ip** command does not show that the control plane is programmed. Actually, there is no entry for the control plane policy in the output.

- CSCsi72758

  Symptoms: Clear inbound multicast traffic can not get to VPNSPA for processing.

  Conditions: This symptom occurs under the following conditions:

  - in crypto connect mode only
  - no encryption and decryption
  - multicast traffic is going through a “ifvlan”

  Workaround: There is no workaround.

- CSCsj01961

  Symptoms: A router may not boot and may generate an :INSUFFICIENT MEMORY” error message.

  Conditions: This symptom is observed on a Cisco 7600 series that has an RSP720 when the ifIndex table is corrupt, preventing SNMP from initializing because SNMP attempts to use the ifIndex table from NVRAM.

  Workaround: There is no workaround.

- CSCsj27811

  Symptoms: A supervisor engine may crash because of a low memory condition that is caused by an Ethernet Out of Band Channel (EOBC) buffer leak and a big buffer leak.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch that runs Cisco IOS Release 12.2(18)SXF9 but could also affect a Cisco 7600 series router that runs Release 12.2SR.

  Workaround: There is no workaround.

- CSCsj35776

  Symptoms: Some PVCs may remain inactive after an ATM SPA has been reloaded.

  Conditions: This symptom is observed on a Cisco 7600 series when the ATM SPA is configured with OAM-managed PVCs and when these are many PVCs.

  Workaround: Increase the *down-count* and *retry-frequency* OAM management arguments for the affected PVCs by using the **oam retry** command.

  Alternate workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the ATM interface with the affected PVCs.

- CSCsj36327

  Symptoms: A SPA-4XOC48POSRPR may not come up after a reload.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA3.

  Workaround: Enter the **hw-module module** *slot* **reset** command for the slot in which the affected SPA is installed.

- CSCsj36477

  Symptoms: When you enter the **shutdown** command on an interface of an OC-192 SPA, the FRR traffic loss may last about 120 ms.

  Conditions: This symptom is observed on a Cisco 7600 series that has a SIP-600 in which an OC-192 SPA is installed.

  Workaround: There is no workaround.

  Further Problem Description: When you physically remove the cable on the Cisco 7600 series, the FRR traffic loss may last only about 2-3 ms. Similarly, when you shut down the remote interface end, which is also a OC-192 SPA interface that is installed in a SIP-600 on a Cisco 12000 series, the FRR traffic loss may last only about 2-3 ms.

- CSCsj37071

  Symptoms: All E1 interfaces on a PA-MC-E3 port adapter may flap continuously even after the traffic has been stopped.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that have a PA-MC-E3 port adapter when you configure 16 or 128 channel groups on each time slot (that is, time slots 1-31) and then generate traffic just above line rate traffic through all the channel groups. Note that the symptom is not platform-specific.

  Workaround: Stop the traffic and reset the E3 controller of the PA-MC-E3 port adapter.

- CSCsj43677

  Symptoms: When you remove the standby supervisor engine, the active supervisor engine may crash and reload.

  Conditions: This symptom is observed on a Cisco 7600 series that has dual Supervisor Engine 720 modules that are configured for SSO.

Workaround: There is no workaround.

- CSCsj47546

  Symptoms: When an interface of a POS SPA detects a Payload Label Mismatch-Path (PLM-P), it may generate a Remote Defect Indication-Path (RDI-P) to the far end. This is improper behavior.

  Conditions: This symptom is observed on a Cisco 7600 series that has a SPA-2XOC3-POS, SPA-4XOC3-POS, SPA-1XOC12-POS, or SPA-1XOC48POS/RPR.

  Workaround: There is no workaround.

  Further Problem Description: Per the Bellcore GR-253 standard, RDI-P must not be transmitted to the far end when the interface detects PLM-P.

- CSCsj55865

  Symptoms: When you shut down an interface that is protected by FRR, a client API error may occur, and the following error message and a traceback may be generated:

  ```
  %LSD_CLIENT-3-CLIENTAPI: Client API error
  ```

  Conditions: This symptom is observed when an MLPS traffic engineering (TE) backup path is configured on the interface and when MPLS TE tunnels are not globally configured and enabled.

  Workaround: Configure and enable MPLS TE tunnels globally.

- CSCsj69176

  Symptoms: When you enter the **standby use-bia** command on an interface and when the HSRP status changes from active to standby on the interface or when HSRP is disabled on an interface that was previously in the active state, the MAC address of the interface is removed from the L2 table. This situation may disrupt L3 connectivity through the interface.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA, 12.2(33)SRA1, 12.2(33)SRA2, 12.2(33)SRA3, 12.2(33)SRA4, 12.2(33)SRB, or 12.2(33)SRB1.

  Workaround: To prevent the symptom from occurring, do not enter the **standby use-bia** command. When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface to restore the MAC address.

  Further Problem Description: Cisco IOS Release 12.2(33)SRA is developed for and intended to run on Cisco 7600 series routers. We do not encourage you to run this release on Cisco Catalyst 6500 series switches. However, if you do run Cisco IOS Release 12.2(33)SRA, 12.2(33)SRA1, 12.2(33)SRA2, 12.2(33)SRA3, or 12.2(33)SRA4 on a Cisco Catalyst 6500 series switch, the symptom may occur.

- CSCsj76268

  Symptoms: When an MFR interface is configured to autosense LMI, the interface may not recover when the T1 links go down or when the interface is wedged.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and a Cisco 7600 series router that are configured with an OSM-12CT3/T1 Optical Services Module.

  Workaround: Configure the LMI type on both the DTE and the DCE. Also, entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the MFR interface may correct the symptom.

  Further Problem Description: Following are the debugs:

  ```
  lmi autosense on by default
  interface MFR1
  ```

```
frame-relay intf-type dce

Debug frame lmi
MFR1(up): DCE LMI timeout
MFR1: Invalid LMI type 1
MFR1(down): DCE LMI timeout
MFR1: Invalid LMI type 1
MFR1: Invalid LMI type 1
MFR1(down): DCE LMI timeout
MFR1: Invalid LMI type 1
MFR1(down): DCE LMI timeout
MFR1: Invalid LMI type 1
MFR1: Invalid LMI type 2
MFR1(down): DCE LMI timeout
```

- CSCsj91961

  Symptoms: When you first create the channels for an E3 interface in a particular order on the active supervisor engine and then the standby supervisor engine is reloaded, the ifNumber objects on the active and standby supervisor engines do not match. This situation prevents proper forwarding on the E3 interface after a switchover.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with an Enhanced FlexWAN.

  Workaround: Reload the router after you have configured the channels for the E3 interface.

- CSCsk08765

  Symptoms: When you add the first link to a multilink or MFR bundle, a bus error crash may occur, and the following error message is generated:

  TLB (load or instruction fetch) exception, CPU signal 10

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA, Release 12.2(33)SRB1, or Release 12.2SXF when you first have attached a policy map to the multilink or MFR interface and then have added the first link to the bundle.

  Workaround: First, add the required number of links to the multilink or MFR interface. Then, attach the service policy to the multilink or MFR interface.

- CSCsk14208

  Symptoms: A WAN line card or module that is configured for WCCP Redirection via the **ip wccp web-cache redirect {out | in}** interface configuration command may not redirect packets to the Cache Engine after an OIR has occurred or after the line card or module has been reloaded.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when WCCP redirection is applied to the interfaces that are configured on the WAN line card or module.

  Workaround: Remove and re-apply the WCCP Redirection configuration to the affected WAN interfaces by entering the **no ip wccp web-cache redirect {out | in}** interface configuration command followed by the **ip wccp web-cache redirect {out | in}** interface configuration command.

  Alternate Workaround: Delete and configure WCCP Redirection globally on the router by entering the **no ip wccp web-cache** router configuration command followed by the **ip wccp web-cache** router configuration command.

- CSCsk16974

  Symptoms: The following error message may be generated on a Supervisor Engine 2 or a line card that functions in bus mode:

  ```
  %PM_SCP-SP-2-LCP_FW_ERR_INFORM: Module 1 is experiencing the following error:
  Bus Asic #0 out of sync error
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router and may occur with a Supervisor Engine 2 or one of the following line cards:

  - 6516-GBIC
  - 6516-GE-TX
  - 6501-10GEX4
  - 6502-10GE
  - 6548-GE-TX
  - 6548-RJ-45
  - 6548-RJ-21
  - 6524-100FX-MM

  Workaround: There is no workaround.

  Further Problem Description: A large amount of traffic may causes the bus ASIC to be flow-controlled. This situation improperly triggers a patch that causes the out-of-sync behavior.

- CSCsk17205

  Symptoms: MFR LMI packets are consistently send through the serial interface that is associated with the MFR interface, instead of the MFR itself. You can verify this situation by enabling debugs:

  ```
  debug frame-relay lmi
   debug packet ----> CPU sensitive
  ```

  Because of this situation, when the LMI type is changed to another type, out- of-sequence problems may occur at the remote end.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with an Optical Services Module (OSM).

  Workaround: There is no workaround.

- CSCsk49151

  Symptoms: A policy map with MPLS EXP ingress marking attached to a non-EoMPLS VLAN is removed when the router is reloaded.

  Conditions: This symptom is observed on a Cisco 7600 series after you have reloaded the router.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, re-attach the policy map to the VLAN interface.

- CSCsk73104

  Cisco IOS contains multiple vulnerabilities in the Data-link Switching (DLSw) feature that may result in a reload or memory leaks when processing specially crafted UDP or IP Protocol 91 packets.

  Cisco has released free software updates that address these vulnerabilities. Workarounds are available to mitigate the effects of these vulnerabilities.

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

- CSCsk79031

  Symptoms: IP Internetworking may not function on a Supervisor Engine 720. For example, traffic may not pass from an EoMPLS VC on a Gigabit Ethernet interface to a serialATM interface.

  Conditions: This symptom is observed on a Cisco 7600 series when a packet is recirculated, for example, because a service policy is attached to the core-facing interface. The symptom is not related to the specific core- facing line card, but the workaround is.

  Workaround: Avoid recirculation of packet in direction from CE towards the core. For example, when service causes recirculation, service policy has to be removed from core interfaces.

Resolved Caveats—Cisco IOS Release 12.2(33)SRA5

Cisco IOS Release 12.2(33)SRA5 is a rebuild release for Cisco IOS Release 12.2(33)SRA. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRA5 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsi77983

  Symptoms: When NetFlow attempts to access a FIB source that is not present in the FIB, the router may crash.

  Conditions: This symptom is observed on a Cisco router that is configured with VLAN interfaces and virtual templates when a FIB source that is related to a virtual interface is not present in the FIB because of severe interface flaps.

  Workaround: There is no workaround.

- CSCsj44081

  Cisco IOS software has been enhanced with the introduction of additional software checks to signal improper use of internal data structures. This enhancement was introduced in select Cisco IOS software releases published after April 5, 2007.

  Details: With the new enhancement in place, Cisco IOS software will emit a "%DATACORRUPTION-1-DATAINCONSISTENCY" error message when it detects an inconsistency in its internal data structures. This is a new error message. The following is an example.

  ```
  The %DATACORRUPTION-1-DATAINCONSISTENCY error message is preceded by a timestamp
  May 17 10:01:27.815 UTC: %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```

  The error message is then followed by a traceback.

  It is important to note that this error message does not imply that packet data is being corrupted. It does, however provide an early indicator of other conditions that can eventually lead to poor system performance or an IOS restart.

  Recommended Action: Collect **show tech-support** command output and open a service request with the Technical Assistance Center (TAC) or designated support organization. Pay particular attention to any other error messages or error symptoms that accompany the "%DATACORR UPTION-1-DATAINCONSISTENCY" message and note those to your support contact.

IP Routing Protocols

- CSCei93982

  Symptoms: A router that is configured for NAT may crash.

  Conditions: This symptom is observed when an application uses two well-known ports: one for the source and the other for the destination. After the outgoing translation is created, on return, when the previous source port is used as the destination, NAT may use an incorrect algorithm.

  For example, when a PPTP session is initiated to well-known port 1723 from source port 21 (FTP), then the outgoing packet creates a FTP translation. (Look at the source information when going from in to out). When the packet is returned, look again at the source information to see what kind of packet is returned. In this situation, with source port 1723, NAT assumes that the packet is a PPTP packet, and then attempts to perform PPTP NAT operations on a data structure that NAT has built for a FT P packet, causing the router to crash.

  Workaround: There is no workaround.

- CSCej20707

  Symptoms: The CPU usage may be high, and an IGP (OSPF or IS-IS) adjacency may drop when PIM sparse mode (PIM-SM) stress traffic is being processed.

  Conditions: This symptom is observed on a Cisco router that connects to a receiver and that has 60,000 (s,G) join messages. The symptom occurs when you enter the **show ip mroute count** command or when there is an abrupt increase in multicast groups.

  Workaround: Do not enter the **show ip mroute count** command. Rather, enter the **show ip mroute count terse** command. Increase multicast groups gradually to avoid high CPU usage. In addition, the following actions may also help to alleviate the symptoms:

  - Enter the **ip pim register-rate-limit** command on the first hop.
  - Enter the **ip pim fast-register-stop** on the PIM-RP.
  - Disable RP rate-limiting commands on the PIM-RP and first hop.

- CSCsb96034

  Symptoms: Routes redistributed from other routing protocols to BGP will be deleted and re-added after an NSF switchover, potentially causing traffic to go down for a long period of time.

  Conditions: This symptom may occur when the route is redistributed from other routing protocols (such as OSPF, ISIS, EIGRP) to BGP.

  Workaround: There is no workaround.

- CSCsd63038

  Symptoms: An MDT address-family session in a BGP environment may not come up between two PE routers. This situation prevents the tunnel interface from being shown in the output of the **show ip pim vrf** *vrf-name* **neighbor** command on one of the PE routers.

  Conditions: This symptom is observed on PE routers that are configured for Multicast VPN and that have the following commands enabled:

  address-family ipv4 mdt

  neighbor *neighbor-ip-address* **activate neighbor**

  neighbor *neighbor-ip-address* **send-community extended**

  Workaround: Reconfigure the **address-family ipv4 mdt** command in the BGP environment.

- CSCse92050

  Symptoms: A router may reload unexpectedly when a routing event causes multicast boundary to be configured on a Reverse Path Forwarding (RPF) interface.

  Conditions: This symptom is observed on a Cisco platforms that is configured for PIM.

  Workaround: Remove multicast boundary from the configuration.

- CSCsg55209

  Symptoms: When BGP updates are received, stale paths are not removed from the BGP table, causing the number of paths for a prefix to increase. When the number of BGP paths reaches the upper limit of 255 paths, the router resets.

  Conditions: This symptom is observed on a Cisco router when the **neighbor soft-reconfiguration inbound** command is enabled for each BGP peer.

  Workaround: Remove the **neighbor soft-reconfiguration inbound** command. A router that runs a Cisco IOS software image that has a route refresh capability, storing BGP updates is usually not necessary.

- CSCsh53926

  Symptoms: A router may crash because of a bus error in the OSPF process.

  Conditions: This symptom is observed on a Cisco router that is configured for incremental SPF (ISPF) and that functions in a network with MPLS TE tunnels.

  Workaround: Remove the ISPF configuration.

- CSCsi49948

  Symptoms: The local BGP MDT prefix may be missing.

  Conditions: This symptom is observed on a Cisco router that has the **mdt default** *group-address* command enabled under a VRF configuration and occurs after you have entered the **clear ip bgp *** command.

  Workaround: Disable and re-enable the **mdt default** *group-address* command.

- CSCsj25841

  Symptoms: A BGP router may not send the default route to its neighbor.

  Conditions: This symptom is observed when the **neighbor default-originate** command is conditionally configured with a route map and when the matching route is installed into the RIB by BGP itself.

  Workaround: There is no workaround.

ISO CLNS

- CSCsg40507

  Symptoms: BFD may not come up when an IP address on an interface is changed and when IS-IS is configured as the routing protocol.

  Conditions: This symptom is observed only when you first enter the **router isis** command and then enter the **bfd all-interfaces** command.

  Workaround: Unconfigure BFD, change the IP address, and then reconfigure BFD.

- CSCsi57971

  Symptoms: IS-IS may not advertise the prefix of a passive interface to the IS-IS database in a local router.

  Conditions: This symptom is observed on a Cisco router when you shut down an interface (for example, G9/1/1) of a 5-port GE SPA (SPA-5X1GE) that is installed in a SIP-600, replace the SPA-5X1GE with another card, and then enter the **no shutdown** interface configuration command on the interface at the same location (G9/1/1) on the new card. In this situation, the prefix for the interface (G9/1/1) is not advertised.

  Possible Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

Miscellaneous

- CSCek55987

  Symptoms: New Xconnect VCs do not function, causing packets that are sent from an OSM to be dropped. Note that packets that arrive on the OSM are not affected.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA4 when a VLAN-based EoMPLS is used with an uplink that is configured on a subinterface of an OSM and occurs only when you attach a service policy to the main interface of the OSM before you configure Xconnect.

  Workaround: Configure Xconnect before you attach the service policy to the main interface of the OSM. Note that the symptom does not occur in Release 12.2(33)SRA3 and Release 12.2SXF.

- CSCek65087

  Symptoms: A traceback may be generated on the supervisor engine when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a tunnel interface.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR.

  Workaround: There is no workaround.

- CSCek66164

  Symptoms: A router may hang briefly and then may crash when you enter any command of the following form:

  show ... | redirect rcp:....

  Conditions: This symptom is observed when Remote Copy Protocol (RCP) is used as the transfer protocol.

  Workaround: Use a transfer protocol other than RCP such as TFTP or FTP.

  Further Problem Description: RCP requires delivery of the total file size to the remote host before it delivers the file itself. The output of a **show** command is not an actual file on the file system nor is it completely accumulated before the transmission occurs, so the total file size is simply not available in a manner that is compatible with RCP requirements.

- CSCsb57042

  Symptoms: While running a health monitoring diagnostics test, the supervisor engine may crash because of an illegal memory access and generate a "%SYS-SP-3-OVERRUN" error message.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that run Cisco IOS Release 12.2(18)SXF4 and on a Cisco 7600 series router that runs Cisco IOS Release 12.2(33)SRA3. The symptom may also affect other releases. The symptom occurs when the firmware of the module that is being tested reports more errors than an SCP message can carry, causing the health monitoring test to access unauthorized memory outside the SCP message.

Workaround Enter the **no diagnostic monitor module** *module-num* **test** *test-id* command for the affected module.

- CSCsb79306

  Symptoms: Setting the cbeDot1dTpVlanAgingFromGlobal from “false” to “true” may cause the standby supervisor engine to reload unexpectedly.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have redundant Supervisor Engine 720 modules that function in SSO mode when the following sequence of events occurs:

  1. USe the CLI to configure a VLAN, for example, VLAN 50:
  2. SNMP creates an entry cbeDot1dTpVlanAgingFromGlobal.50 with the value set to “true”.
  3. Manually set the value for cbeDot1dTpVlanAgingFromGlobal.50 from “true” to “false”.
  4. USe the CLI to delete VLAN 50.
  5. When you initiate a mibwalk for cbeDot1dTpVlanAgingFromGlobal, the entry for VLAN 50 is still present.
  6. Manually set the value for cbeDot1dTpVlanAgingFromGlobal.50 from “false” to “true”.

  This last event causes the standby supervisor engine to reload unexpectedly.

  Workaround: Do not use or limit the use of cbeDot1dTpVlanAgingFromGlobal.

- CSCsc89932

  Symptoms: A switch or router may crash when you enter the **show diagnostic sanity** command.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsc95875

  Symptoms: After multiple SSO switchovers occur on a Cisco 7600 series, an OSM or FlexWAN module may be reset by the switch processor because of a keepalive or SCP failure.

  The same symptom may occur while toggling hardware switching by entering the **no mls switching** command followed by the **no mls switching** command.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR and that has a non-fabric-enabled LAN card in its chassis.

  Workaround: There is no workaround.

- CSCsd31503

  Symptoms: Some protocol packets such as OSPF, EIGRP, MPLS LDP, BGP, and IS-IS may be dropped at the Route Processor (RP) because SPD classifies them as lower-priority packets.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when there are a number of routing protocols running with a very large topology and when rapid topology changes or changes in link states occur, causing more traffic to be processed by the RP.

Workaround: Increase the priority of the protocol packets by entering the configuration stated below, in which 0 indicates a lower priority and 7 indicates a higher priority and in which the following levels are used for packet classification:

- 0-1, indicating that the packet is to be dropped
- 2-4, indicating that as a last resort the packet is to be dropped
- 5-7, indicating that the packet should be the last one to be dropped.

Priority level 5-7 is best suitable for protocol packets.

```
Router(config)#mls qos protocol ospf precedence 6
 Marking will work on the packet which comes from untrusted port
Router(config)#mls qos protocol ?
  isis
  eigrp
  ldp
  ospf
  rip
  bgp
  ospfv3
  bgpv2
  ripng
  neigh-discover
  wlccp
  arp


Router(config)#mls qos protocol eig
Router(config)#mls qos protocol eigrp ?
  pass-through  pass-through keyword
  police        police keyword
  precedence    change ip-precedence(used to map the dscp to cos value)
Router(config)#mls qos protocol eigrp pr Router(config)#mls qos protocol eigrp
precedence 6  Marking will work on the packet which comes from untrusted port
```

- CSCsf23115

  Symptoms: After the fan tray has failed, the system can not determine if the fan tray is an original fan (FAN1) or high-speed fan (FAN2).

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that hare configured with a Supervisor Engine 720.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur on a Cisco Catalyst 6504-E or Cisco Catalyst 6509 NEB that are configured with an E-FAN.

- CSCsg00252

  Symptoms: A Cisco 7600 series may generate the following error message:

  ```
  MSC-RPDF ASSERTION FAILED 0
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for multicast traffic when the replication mode is changed.

  Workaround: There is no workaround.

- CSCsg41552

  Symptoms: A module does not come online after excessive fabric errors followed by a power-cycle of the module.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router. The symptom occurs because the Serial Control Protocol (SCP) fails to download. The following modules are affected:

  - WS-X6704-10GE
  - WS-X6748-GE-TX
  - WS-X6724-SFP
  - WS-X6748-SFP
  - WS-X6708A-10GE

  Workaround: Manually reset the power of the module by entering the **hw-module slot** *slot-number* **reset** command.

- CSCsg47039

  Symptoms: After a Fast Reroute (FRR) event and multiple failure situations have occurred, any of the following line cards or port adapters may crash:

  - SIP-600
  - 2-port Ethernet Services line card (7600-ES20-10G)
  - 20-port Ethernet Services line card (7600-ES20-GE)

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for MPLS Traffic Engineering Fast Reroute--Link Protection when the line card or port adapter is processing incoming traffic from the MPLS core and when the following sequence of events occurs:

  - You remove the protected TE tunnel configuration from the protected interface.
  - You add back the protected TE tunnel configuration to the same interface.
  - You clear the fault that caused the FRR event.

  The crash occurs after OSPF and LDP are negotiated through the protected interface.

  Workaround: After the FRR event has occurred, do not remove the protected TE tunnel configuration from the protected interface.

- CSCsg70474

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsh25976

  Symptoms: There are two symptoms:

  1. 1) The threshold of the fan-fail sensor of the power supply may not be updated correctly, and the following error message may be generated:

     power-supply incompatible with fan: N/A

     The value should not be “N/A” but “OK”.

  2. 2) The threshold of the fan-fail sensor of the power supply may get be added when power supply is detected. For example, information about the fan-fail sensor of the power supply may not be shown in the output of the **show environment alarm thresholds power-supply** command.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: Initiate a Stateful Switchover (SSO). After the SSO, the symptom no longer occurs.

- CSCsh89826

  Symptoms: When a QoS service policy is applied to a serial interface, the rate that is provided to the default queue may drop to unexpectedly low values.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(31)SRA1 with a SPA-4XCT3/DS0 that in installed in a SIP-200. The following is an example of a configuration in which the symptom occurs:

```
class-map match-all MGCP
  match ip precedence 4
class-map match-all RTP
  match ip precedence 5

policy-map TEST1
  class RTP
    priority percent 88
  class MGCP
    bandwidth percent 10

     interface Serial2/0/0/17:0
      ip address 10.1.0.13 255.255.255.252
      encapsulation ppp
      load-interval 30
      service-policy output TEST1
```

  In this configuration, when there are eight G.711 calls and an FTP file is sent, the throughput is around 30 Kbps of application data for the FTP file. Considering the output service policy and the fact that the priority class does not consume the bandwidth, this throughput rate is very low. Moreover, after a few minutes of operation, the throughput rate drops to about 2 Kbps even though the rate that is provided in the priority queue has not changed. When the traffic is removed from the priority queue, the default queue continues to serve traffic at the reduced rate of only a few Kbps even though the full T1 line is now available.

Workaround: Remove the service policy from the interface to enable the data traffic to resume flowing at a normal rate.

- CSCsi41791

  Symptoms: A buffer memory leak may cause a SPA-IPSEC-2G to crash. When this situation occurs, the following error messages are generated in the logs:

  ```
  SPA_IPSEC-3-PWRCYCLE: SPA (<slot/subslot>) is being power-cycled (Module not
  responding to keep-alive polling)
  ```

  ```
  SPA_OIR-3-RECOVERY_RELOAD: subslot <slot/subslot>: Attempting recovery by reloading
  SPA
  ```

  ```
  ACE-6-INFO: SPA-IPSEC-2G[<slot/subslot>]: Crypto Engine X going DOWN
  ```

  Conditions: This symptom is observed rarely on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when GRE fragments are reassembled by the SPA-IPSEC-2G and when the length of the IP packet after GRE decapsulation is more than 9126 bytes.

  Workaround: To prevent the symptom from occurring, proactively reload the SPA-IPSEC-2G outside of business hours by entering the **hw-module subslot** *slot/subslot* **reload** command.

- CSCsi46469

  Symptoms: The CBQoSMIB may generate inaccurate results: a manual snmpwalk of the CBQoSMIB may fail with errors that indicate “OID not increasing.”

  Conditions: This symptom is observed on a Cisco 7609 that runs Cisco IOS Release 12.2(33)SRA2 and that is configured for QoS.

  Workaround: There is no workaround.

- CSCsi49520

  Symptoms: A medium buffer leak may occur on an MSFC.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that function as a PE router after an SSO has occurred.

  Workaround: There is no workaround.

- CSCsi52209

  Symptoms: A SIP-600 may crash, and the following error message may be generated:

  ```
  %PXF-DFC1-2-FAULT: T0 OHB Exception: SLIP FIFO full WARNING: PXF Exception:
  mac_xid=0x40000 ***
  PXF OHB SLIP FIFO Full %SIP600-DFC1-2-UNRECOVERABLE_FAILURE: SIP-600 Unrecoverable
  Failure
  ```

  Conditions: This symptom is observed on a Cisco 7600 series.

  Workaround: There is no workaround.

- CSCsi60004

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsi69350

  Symptoms: The RP on the standby supervisor engine may crash during the boot process when you upgrade the ROMmon of the RP on the standby supervisor from the active supervisor engine.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have redundant Supervisor Engine 720 modules that function in RPR mode when you upgrade the ROMmon of the RP on the standby supervisor from the active supervisor engine by entering the **upgrade rom-monitor slot** *slot-num* **rp file** *filename* command.

  Workaround: There is no workaround.

- CSCsi75566

  Symptoms: Packets may be dropped on a Fast ReRouting (FRR) backup tunnel.

  Conditions: This symptom is observed on a Cisco router when the primary MPLS TE tunnel is protected by a backup tunnel and when the protected tunnel interface is a subinterface that goes administratively down.

  Workaround: There is no workaround.

  Further Problem Description: Process-switched traffic (such as traffic that originates from the router itself or a ping with a record option) is not impacted.

- CSCsi86396

  Symptoms: Two subinterfaces may have the same CEF interface index.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when the following configuration sequence occurs:

  1. Create subinterface 1, 2, and 3.
  2. Delete subinterface 1.
  3. Create subinterface 4.
  4. Enable subinterface 1.

  In this situation, subinterface 1 and 4 may have the same CEF IDB.

  Workaround: There is no workaround. You must reload the platform to clear the symptoms.

- CSCsi89136

  Symptoms: When you remove and re-add a working VRF instance, the IP connectivity to VRF sites may break.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA2, that functions as a PE router and a Layer 3 switch, and that connects to another PE router that has VRF instances.

  Workaround: There is no workaround.

- CSCsi98993

  Symptoms: When you attempt an FPD downgrade on an ATM SPA, an error message similar to the following may be generated, and the SPA may be disabled:

  ```
  %FPD_MGMT-3-FPD_UPGRADE_FAILED: I/O FPGA (FPD ID=1) image upgrade for SPA- 4XOC3-ATM
  card in subslot 3/0 has FAILED.
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with an SPA-2XOC3-ATM, SPA-4XOC3-ATM, SPA-1XOC12-ATM, or SPA-1XOC48-ATM.

  With an SPA-2XOC3-ATM, SPA-4XOC3-ATM or SPA-1XOC12-ATM, the symptom occurs when the hardware version is newer than version 1.0 and when the downgrade FPD image version is older than version 1.26.

  With an SPA-1XOC48-ATM, the symptom occurs when the hardware version is newer than version 1.0 and when the downgrade FPD image version is older than version 0.15.

  Workaround: There is no workaround to downgrade the FPD for these cases, but the symptom does not actually corrupt the FPD image on the SPA. You can bring up SPA again by entering the **hw-module subslot** *slot-number/subslot -number* **reload** command.

- CSCsj37398

  Symptoms: A CoS value may be incorrectly changed.

  Conditions: This symptom is observed on a cisco 7600 series when a register is not initialized properly, causing traffic to be marked to a random CoS value.

  Workaround: There is no workaround.

- CSCsj59997

  Symptoms: When a VTI is created, traffic that is generated by the Route Processor such as a ping and routing protocol hello messages may be dropped at the interface level.

  The output of the **show interface tunnel** *number* command shows the output drops:

  ```
  router#sh int tu 1 | i drop
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 26
  router#
  ```

  The output of the **show ip traffic** command shows that the number of "encapsulation failed" increases:

  ```
  router#sh ip traff | i Drop
    Drop:  26 encapsulation failed, 0 unresolved, 0 no adjacency
  router#
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with a SPA-IPSEC-2G when both of the following conditions are present:

  – The tunnel destination is not directly connected to the switch or router.

  – Proxy ARP is not enabled on the next-hop router to the tunnel destination.

  Workaround: Create a dummy ARP entry for each VTI tunnel destination, as in the following example:

  ```
  arp <tunnel destination ip> 1111.1111.1111 arpa.
  ```

- CSCuk61396

  Symptoms: WCCP service redirection may not work. In particular, packets that are rejected by a third-party vendor appliance device and are returned to the router for normal forwarding may be discarded.

Conditions: This symptom is observed on a Cisco router when NAT or Cisco IOS Firewall features are enabled on the same interfaces that have WCCP enabled.

Workaround: There is no workaround.

Wide-Area Networking

- CSCsi70727

  Symptoms: A fragment size may be incorrect for Link Fragmentation and Interleaving (LFI) over Frame Relay.

  Conditions: This symptom is observed on a Cisco router that is configured for Multilink PPP (MLP) over Frame Relay when a script tests LFI over Frame Relay by looking for a fragment size in the output of the **show ppp multilink interface** *number* command.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRA4

Cisco IOS Release 12.2(33)SRA4 is a rebuild release for Cisco IOS Release 12.2(33)SRA. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRA4 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCdy11174

  Symptoms: Some object of the ciscoFlashCopyTable and ciscoFlashMiscOpTable cannot be read after row creation.

  Conditions: This symptom is observed for any newly created rows in these tables.

  Workaround: Objects will become readable immediately after being set. Additionally, rows can still be activated in these tables even if all objects cannot be read. Any objects that cannot be read contain their MIB-defined default value.

- CSCeh85133

  Symptoms: A memory leak may occur when an SNMP trap is sent to a VRF destination. The output of the **show processes memory** command shows that the memory that is held by the process that creates the trap increases, and eventually causes a MALLOC failure. When this situation occurs, you must reload the platform.

  Conditions: This symptom is platform-independent and occurs in a configuration in which at least one VRF destination has the **snmp-server host** command enabled.

  Workaround: Ensure that no VRF is associated with the **snmp-server host** command.

- CSCsc09336

  Symptoms: When you enter the **show memory detailed** command, memory leaks in the process that this command is applied to.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that are configured for Cisco IOS Software Modularity.

  Workaround: There is no workaround.

- CSCsd23056

  Symptoms: Reverse Telnet may not function.

  Conditions: This symptom is observed when AAA authentication is enabled for the asynchronous line over which you attempt to establish a reverse Telnet connection. The AAA authentication prompt takes the console output as input for the AAA authentication process, causing a login failure for reverse Telnet.

  Workaround: There is no workaround.

- CSCse80032

  Symptoms: An SNMP Manager that uses SNMPv3 may not resynchronize the timer for the SNMP engine after the router has been reloaded.

  Conditions: This symptom is observed on Cisco Catalyst 6000 series switch and Cisco 7600 series router that have been reloaded and occurs because a parameter is incorrectly set in the REPORT message, causing a mediation device to register an SNMP timeout instead of a reload.

  Workaround: You may be able to restart the SNMP Manager to force the timer for the SNMP engine to resynchronize. Note, however, that doing so causes a 100-percent outage for all wiretaps that are served by the SNMP Manager. If you cannot restart the SNMP Manager, there is no workaround.

EXEC and Configuration Parser

- CSCsd32923

  Symptoms: A router may unexpectedly reload with a bus error when you enter a command while the command buffer is full of white space.

  Conditions: This symptom is observed when you enter a partial command and when the tab key is used while the command buffer is full.

  Workaround: There is no workaround.

IBM Connectivity

- CSCse17611

  Symptoms: When DLSw Ethernet Redundancy is configured, circuits may be established through the wrong switch.

  Conditions: This symptom is observed in the following configuration:

  - Clients are connecting to MAC A.
  - Mapping statements are configured so that “Switch 1” has a mapping of MAC A = MAC A and “Switch 2” has a mapping of MAC B = MAC A.

  The output of the **show dlsw transparent map** command shows that “Switch 1” has the active mapping and that “Switch 2” has the passive mapping. All circuits should be established on “Switch 1”, but instead they are established on “Switch 2”.

  The outputs of the **show dlsw trans neighbor** and **show dlsw trans map** commands show correct information, but the output of the **show dlsw cir cache** command shows state “negative” on “Switch 1” and state “positive” on “Switch 2”.

  Workaround: There is no workaround. Note that all circuits are up and running, but they just go through the wrong router.

Interfaces and Bridging

- CSCsd94687

  Symptoms: The output of the **show vlans** *vlanID* shows the wrong counters. The counters do not match the SNMP counters.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router.

  Workaround: Use only the SNMP counters.

IP Routing Protocols

- CSCed84633

  Symptoms: The *interface-type* and *interface-number* arguments in the **distribute-list** address family configuration command do not function.

  Conditions: This symptom is observed on a Cisco platform that integrates the fix for caveat CSCea59206. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCea59206. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

  Workaround: There is no workaround.

  Further Problem Description: The fix for CSCed84633 re-enables the *interface-type* and *interface-number* arguments in the **distribute-list** address family configuration command for both VRF interfaces and non-VRF interfaces.

- CSCei29944

  Symptoms: A CE router that has L2TP tunnels in an MPLS VPN environment with about 1000 VRFs may crash and generate the following error message:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x50766038
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(32)S and that functions as a CE router when BGP neighbors are unconfigured via the **no neighbor** *ip-address* command while the **show ip bgp summary** command is entered from the Aux console. The symptom is not release-specific and may also affect other releases.

  Workaround: There is no workaround.

- CSCsd99760

  Symptoms: The routing table is not updated with an IP route for a prefix for a properly connected routed interface even though the CEF table shows a receive entry for the same prefix at both the RP and the SP.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when the following conditions occur:

  1. The IP routing process iprouting.iosproc is restarted.
  2. You change a switch virtual interface (SVI) port to a routed port.
  3. You configure the port with the same IP address as the address that was associated with the SVI port.
  4. You make the port active by entering the **no shutdown** command.

In this situation, the routing table is not updated with the IP route for the prefix for the new routed port.

Workaround: Restart the IP routing process iprouting.iosproc once more.

- CSCse05031

  Symptoms: The **neighbor default-originate** command does not function properly when the **route map** keyword and *map-name* argument are defined.

  Conditions: This symptom is observed when the target route that is specified in the route map is added or removed from the routing table after the BGP session has already been established.

  Workaround: Clear and re-establish the BGP neighbor.

- CSCse41484

  Symptoms: A DMVPN hub receives a few unencrypted GRE packets from a spoke during the negotiation of an IPsec security association (SA).

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for NHRP and that have an IPsec VPN SPA that functions as a spoke in a DMVPN topology.

  Workaround: There is no workaround.

- CSCsf99057

  Symptoms: The OSPF Stub Router Advertisement feature may stop functioning after an RPR+ or SSO switchover has occurred, and the newly active RP does not originate router LSAs with infinity metric as it should do when the **max-metric router-lsa on-startup** router configuration command is enabled.

  Conditions: This symptom is observed on a Cisco router that has dual RPs that function in RPR+ or SSO mode when NSF is not enabled on the router and when the standby RP is in the “Standby-Hot” state.

  Workaround: Do not configure RPR+ or SSO. Rather, configure RPR. If this is not an option, there is no workaround.

- CSCsg43140

  Symptoms: A router may crash during the boot process and return to ROMmon.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that has VPNs configured.

  Workaround: There is no workaround.

ISO CLNS

- CSCse34050

  Symptoms: IS-IS may not advertise a passive interface when it should do so, or IS-IS may advertise a passive interface when it should not do so.

  Conditions: This symptom is observed on a Cisco router when IS-IS misinterprets an interface “shutdown” event as an UP event.

  Workaround: Enable IS-IS on the interface by entering the **ip router isis** command and then make the interface passive by entering the **no ip router isis** command followed by the **passive-interface** *interface-type interface-number* command.

- CSCsf26043

  Symptoms: IS-IS protocol packets may not be classified as high-priority. When this situation occurs during stress conditions and when the IS-IS protocol packets are mixed with other packets, the IS-IS protocol packets may be dropped because of their low-priority.

  Conditions: This symptom is observed on a Cisco platform that is configured for Selective Packet Discard (SPD).

  Workaround: Ensure that DSCP rewrite is enabled and then enter the following command:

  ```
  mls qos protocol isis precedence 6
  ```

Miscellaneous

- CSCeb05456

  Symptoms: A Cisco platform may reset its RP when two simultaneous **write memory** commands from two different vty connections are executed, and messages similar to the following may appear in the crashinfo file:

  ```
  validblock_diagnose, code = 10
  current memory block, bp = 0x48FCC7D8,
  memory pool type is Processor
  data check, ptr = 0x48FCC808
  next memory block, bp = 0x491AC060,
  memory pool type is Processor
  data check, ptr = 0x491AC090
  previous memory block, bp = 0x48FCBBE8,
  memory pool type is Processor
  data check, ptr = 0x48FCBC18
  ```

  The symptom is intermittent and is related to the way NVRAM is accessed.

  Conditions: This symptom is observed on a Catalyst 6000 series Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXD but is platform- and release-independent.

  Workaround: Set the boot configuration to non-NVRAM media such as a disk or bootflash by entering the following commands:

  ```
  boot config disk0:
  filename
  nvbypass
  ```

- CSCeb21064

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCeg02918

  Symptoms: A Cisco router that is configured with an HTTP authentication proxy may reload because of a bus error.

  Conditions: This symptom is observed on a Cisco router that runs a crypto image of Cisco IOS Release 12.3(9) or Release 12.3(10). Note that the symptom is not release-specific.

  Workaround: Disable the HTTP authentication proxy. If this is not an option, there is no workaround.

- CSCeh18195

  Symptoms: Packets that flow to VPNv4 destinations may be dropped for up to one second when the next-hop router clears its IS-IS overload bit after having been rebooted.

  Conditions: This symptom is observed in a MPLS-TE network with one-hop TE tunnels.

  Workaround: There is no workaround.

- CSCeh86935

  Symptoms: As a user of a router, you cannot authenticate or authorize via a TACACS+ server. A TCP SYN that is sent from the router to port 49 of the TACACS+ server carries an incorrect source IP address. Instead of the address that is specified in the **ip tacacs source-interface** *subinterface-name* command, the router uses the default address for login authentication and exec authorization. The nondefault source interface is correctly used for command authorization.

  Conditions: This symptom is observed on a Cisco router that is configured to use a nondefault source interface to connect to a TACACS+ server when there is at least one authentication or authorization method list configured to use one more TACACS+ servers and when the following command sequence is enabled:

  ```
  aaa new-model
  tacacs-server host host-ip-address
  tacacs-server key key
  ip tacacs source-interface subinterface-name
  ```

  Workaround: Remove the **ip tacacs source-interface** *subinterface-name* command.

  Further Problem Description: Protocols other than TACACS+ that use TCP and that are implemented via the sockets library may also use an incorrect source address when they are configured to use a nondefault source interface or address. This situation may cause problems, depending on the configuration of the router, the routing tables, and the configuration of the outside client or server with which the other protocol communicates. In Cisco IOS software images, most services that use TCP, including BGP, are not implemented via sockets but, instead, use a proprietary interface for the TCP protocol, and are not affected.

  Some older versions of TACACS+ do not use sockets. In a Cisco IOS software image with such an older TACACS+ version, TACACS+ is not affected but other services may still be affected.

  Workaround for protocols other than TACACS+: Remove the configuration that specifies a source interface or source address from the router.

- CSCei52830

  Symptoms: A router or switch may not properly function when you enter a message-of-the-day (MOTD) through the **banner motd** *d message d* command because the *d message d* argument of the command may not be synchronized to the standby RP.

Conditions: This symptom is observed on Cisco router or switch that is configured for SSO.

Workaround: Do not enter the **banner motd** *d message d* command.

- CSCej08637

  Symptoms: When you run the Entity-MIB on a redundant system, the standby supervisor engine may reset. When you enter the **show environment status** command on the standby supervisor engine, the module information is not shown, nor are inline power sensors on the VDB shown.

  Conditions: These symptoms are observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured for SSO.

  Workaround: There is no workaround.

- CSCej21698

  Symptoms: A switch or router that is configured for multicast may generate the following error message when stress traffic is sent:

  ```
  %EARL_L2_ASIC-DFC8-4-SRCH_ENG_FAIL: EARL L2 ASIC Search Engine has failed: ios-base
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that functions under stress.

  Workaround: There's no workaround.

- CSCek35417

  Symptoms: When the ROMmon of an RP on a Supervisor Engine 720 resets or reboots or when the platform resets or reboots, the ROMmon may not load the runtime image because of a corrupted NVRAM. When this situation occurs, the following error message is generated:

  ```
  "Warning: Rommon NVRAM area is corrupted. Initialize the area to default values
  Cat6k-Sup720/RP platform with 1048576 Kbytes of main memory"
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have a Supervisor Engine 720 on which the NVRAM is installed on a flash device.

  Workaround: Erase the ROMmon in the NVRAM and set the ROMmon confreg utility to 0x2102, as in the following example:

  ```
  rommon 1 > priv
  rommon 2 > nvram_erase

  Enter in hex value the start address [0x0]:  0xbe000000
  Enter in hex value the test size or length in bytes [0x0]:  0x20000

  rommon 3 > confreg 0x2102
  rommon 4 > reset
  ```

- CSCek47574

  Symptoms: When you enter a **traceroute** command to check the route to an interface that has MPLS enabled, the first hop may be dropped. After the first hop, the **traceroute** command completes normally. Furthermore, for each **traceroute** command, three input errors occur on the MPLS interface.

  Conditions: These symptoms are observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA2 and that is configured with a SIP-400 in which an OC-48 SPA is installed. The symptom occur when the MPLS interface receives packets while the time-to-live (TTL) is set to "0" or "1". The MPLS interface drops these packets.

  Workaround: There is no workaround. However, the symptom does not affect the functionality of the router.

  Further Problem Description: Although the symptom is observed with the **traceroute** command, the packets drops could occur with any application when the TTL is set to "0" or "1".

- CSCek63611

  Symptoms: IPSec SA rekey operations may fail with an IPSec VPN SPA (SPA-IPSEC-2G).

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router for SAs that are established after the SPA-IPSEC-2G has been reloaded.

  Workaround: There is no workaround.

- CSCek66277

  Symptoms: When you run the TestAclDeny diagnostic test, the output of the **show diagnostic content module** *num* command, with the *num* representing the active supervisor engine, shows the test as "N" to denote non-disruptive. This situation is shown in the following example:

  ```
  18) TestAclDeny ----------------------> M**N****A*** 000 00:00:05.00 n/a
  ```

  In reality, the TestAclDeny diagnostic test for the active supervisor engine is a disruptive test because the test may cause traffic forwarding issues and flapping of the first uplink port.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: Do not run the TestAclDeny diagnostic test.

  Further Problem Description: The fix for this caveat sets the flag to "D" to denote disruptive.

- CSCek67100

  Symptoms: A crashdump may not be saved when a SSC-400 crashes.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCek67701

  Symptoms: When an exception occurs on an IPSec VPN SPA (SPA-IPSEC-2G) there is insufficient time to save the crashdump file before the SPA-IPSEC-2G is automatically reset.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat enables the SPA-IPSEC-2G to save the crashinfo file. In turn, the crashinfo file enables you to find the cause of the exception.

- CSCek70058

  Symptoms: An Optical Services Module (OSM) may crash because of a memory corruption.

  Conditions: This symptom is observed when you apply a QoS configuration with WRED.

  Workaround: There is no workaround.

- CSCir00786

  Symptoms: When you attempt to update the startup configuration from a file but the **boot** commands are incorrect or you are unauthorized to enter the **boot** commands, a boot configuration error message should be displayed, but this does not occur.

  Conditions: This symptom is observed on a Cisco router after the startup configuration has been updated by SNMP.

  Workaround: Perform the following tasks:

  1. Copy the startup configuration to the running configuration.

2. Copy the running configuration to the startup configuration.
3. Verify manually that the **boot** commands are indeed correct and use the CLI to update the startup configuration.

- CSCsb45696

  Symptoms: A platform may reload in response to malformed 802.1x EAP traffic.

  Conditions: This symptom is observed on a Cisco Catalyst 3750 that runs Cisco IOS Release 12.2(25)SEC. However, the symptom is both platform- and release-independent.

  Workaround: There is no workaround.

- CSCsb54378

  Symptoms: A router may reload due to software forced crash.

  Conditions: This problem has been observed when initiating a Secure Shell (SSH) session from the router or when copying a file to/from the router via SCP.

  Workaround: Do not initiate SSH or SCP sessions from the router.

  Further Problem Description: This was observed on a Cisco 2811 router that was running Cisco IOS Release 12.4(4)T. Note that the symptom is not platform- or release-specific.

  Prior to the crash, the router logs a series of %SYS-3-CPUHOG messages and will eventually crash with %SYS-2-WATCHDOG. See the following example:

```
%SYS-3-CPUHOG: Task is running for (128004)msecs, more than (2000)msecs
(1426/5),process = Virtual Exec.
-Traceback= 0x41DC8E2C 0x41DC9098 0x41BAA6E0 0x41BA6990 0x41B96B4C 0x41BA6768
0x41BA7490 0x41BA7750
0x41BAC854 0x41BA120C 0x40C27024 0x40C26760 0x41BA203C 0x40C73E58 0x40C926E8
0x41834200
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Virtual Exec.
-Traceback= 0x41A23CC8 0x41BAA3D8 0x41BA6A08 0x41B96B4C 0x41BA6768 0x41BA7490
0x41BA7750 0x41BAC854
0x41BA120C 0x40C27024 0x40C26760 0x41BA203C 0x40C73E58 0x40C926E8 0x41834200
0x418341E4
%Software-forced reload
```

- CSCsb61381

  Symptoms: A router or switch that has an ATA file system may crash when the **dir** *all-filesystems* command is executed.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router. The symptom may occur when a network management tool such as CiscoWorks periodically backs up or restores the vlan.dat file along with the configuration of the system while other periodic scripts execute the **dir** *all-filesystems* command.

  Workaround: Prevent applications such as CiscoWorks from accessing the vlan.dat file.

- CSCsb64767

  Symptoms: When a layer 2 EtherChannel is load-balancing multicast traffic on multiple member ports of a local switch or router, one port may not transmit multicast packets but may drop them. When this situation occurs, the OutMcastPkts counter for this port does not increase.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when an OIR is performed on a line card of the remote switch or router, causing the local port that is a member of the EtherChannel to change its state to link down and then to link up.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on affected member port of the local switch or router. Doing so re-enables multicast forwarding.

- CSCsb66799

  Symptoms: After a router has been reloaded, an URL match statement unexpectedly may be removed from the configuration.

  Conditions: This symptom is observed when the **match protocol http url** *url-string* command is enabled. After the router has been reloaded, this command has disappeared from the configuration.

  Workaround: There is no workaround.

- CSCsb79031

  Symptoms: A Cisco Catalyst 6500 series switch or Cisco 7600 series router may crash when you enter the **clear counters** command.

  Conditions: This symptom is observed when a communication problem occurs with one of the CSMs. Internal communication problems can be reported through an ICC, IPC, or SCP error message such as the following ICC-4-HEARTBEAT message:

  ```
  %ICC-4-HEARTBEAT: Card 6 failed to respond to heartbeat.
  ```

  Workaround: Do not enter the **clear counters** command when an ICC-4-HEARTBEAT message is generated for an CSM.

- CSCsc09892

  Symptoms: A spurious memory access may occur on a supervisor engine.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for SNMP and QoS.

  Workaround: There is no workaround.

- CSCsc19259

  The server side of the Secure Copy (SCP) implementation in Cisco IOS contains a vulnerability that allows any valid user, regardless of privilege level, to transfer files to and from an IOS device that is configured to be a Secure Copy server. This vulnerability could allow valid users to retrieve or write to any file on the device's filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

  The Cisco IOS Secure Copy Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS Secure Copy Server service are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS Secure Copy Client feature.

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml.

- CSCsc33990

  Symptoms: A supervisor engine may unexpectedly reset when the TestSPRPInbandPing as part of the Cisco Generic Online Diagnostics (GOLD) fails for 10 consecutive times.

  The following syslog error messages are typically generated right before the supervisor engine resets, and can also be found in the crashinfo files:

  ```
  %CONST_DIAG-SP-3-HM_TEST_FAIL: Module <slot#> TestSPRPInbandPing consecutive failure
  count:5
  ```

```
%CONST_DIAG-SP-6-HM_TEST_INFO: CPU util(5sec): SP=10% RP=0% Traffic=0%
netint_thr_active[0], Tx_Rate[4412], Rx_Rate[0]

%CONST_DIAG-SP-3-HM_TEST_FAIL: Module <slot#> TestSPRPInbandPing consecutive failure
count:10

%CONST_DIAG-SP-6-HM_TEST_INFO: CPU util(5sec): SP=10% RP=0% Traffic=0%
netint_thr_active[0], Tx_Rate[4652], Rx_Rate[0]

%CONST_DIAG-SP-2-HM_SUP_CRSH: Supervisor crashed due to unrecoverable errors, Reason:
Failed TestSPRPInbandPing
```

Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that run an integrated Cisco IOS software image. The trigger for the symptom may be possible corruption in TCAM entries that are used to perform the TestSPRPInbandPing.

Workaround: Enter the **no diagnostic crash** global configuration command to disable exceptions that are being triggered by failed diagnostic monitoring. However, you should do this with discretion because it may also prevent the system from taking proactive measure to mitigate problems that could impact user traffic.

Further Information: The fix for this caveat is more of an enhancement because it only prevents the system from being over-aggressive in taking exceptions when the TestSPRPInbandPing fails under specific conditions. Therefore, the fix for this caveat does not address all triggers that may cause the TestSPRPInbandPing to fail. Please consult Cisco TAC for further assistance if you experience the same problem after upgrading to a Cisco IOS software image that contains the fix for this caveat.

- CSCsc46105

  Symptoms: The type of service (ToS) value from a Cisco SSL Module (SSLM) for back-end encryption is not carried over but is stripped off.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when the **tos carryover** command is enabled on the SSLM and when the **mls qos** command is enabled in Native IOS. The symptom does not occur when the **mls qos** command is not enabled, nor does it occur for encryption in the direction of the clients.

  Workaround: Disable the **mls qos** command in Native IOS.

- CSCsc56766

  Symptoms: When channel members of an EtherChannel are located on different forwarding engines and when one channel goes down, traffic may be disturbed for six seconds or longer and a control protocol may be adversely affected. The duration of the traffic disturbance depends on the number of VLANs.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch but may also occur on a Cisco 7600 series router.

  Workaround: Place all members of the EtherChannel on the same forwarding engine.

  Alternate Workaround: Limit the number of VLANs on the trunk.

- CSCsc71245

  Symptoms: A router that is connected to several VPN clients may unexpectedly reload because of a CPUHOG condition in the crypto IKMP process followed by a watchdog timeout.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router and occurs about every about 24 hours, which is equal to the IKE lifetime.

  Workaround: There is no workaround.

- CSCsd17641

  Symptoms: A hierarchical service policy may not be attached to a subinterface, and no error message is generated, as if the configuration is ignored. Entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the subinterface or deleting the subinterface does not have any effect.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA2 and that is configured with subinterfaces on a SPA-2X1GE that is installed in a SIP-400.

  Workaround: Do not use a hierarchical service policy.

  Further Problem Description: Debugs of the SIP-400 show that for the subinterfaces that works fine, the SIP-400 received the commands from MQC. For the subinterfaces that do not work, the SIP-400 did not receive any commands to program the queues.

- CSCsd28214

  Symptoms: A Cisco router may crash because of a watch dog timeout while running the RIP routing protocol.

  Conditions: This symptom is observed on a router that runs Cisco IOS Release 12.3(19) when an interface changes state at the exact same time that a RIP route that was learned on this interface is being replaced with a better metric redistributed route. For example, when RIP has learned the 192.168.1.0 network from Fast Ethernet 1/0 interface and then RIP learns the 192.168.1.0 network from a redistributed protocol that has a better metric, the RIP route is removed. However, when during this time the Fast Ethernet 1/0 interface goes down, the router may crash because of a watch dog timeout. Note that the symptom may also affect other releases.

  Workaround: There is no workaround.

- CSCsd70948

  Symptoms: After an SSO switchover occurs, the supervisor engine stops receiving BPDUs and CDPs. You must reload the platform to enable the platform to receive CDP and BPDUs.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when rate-limiting of layer 2 BPDUs is enabled through the **mls rate-limit layer2 pdu** command.

  Workaround: Disable rate-limiting of layer 2 BPDUs by entering the **no mls rate-limit layer2 pdu** command.

- CSCsd71047

  Symptoms: When the MAC address of a local-source address in a NAT configuration is changed, for example because of a failover between NICs, the corresponding NetFlow entry is not updated, causing return traffic to continue to be send to the old MAC address. In turn, this situation causes traffic to be dropped at the destination or to be send to an incorrect interface until the NetFlow entry times out or is cleared.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when either static NAT or dynamic NAT is configured.

  Workaround: Clear the corresponding NetFlow entry by entering the **clear mls netflow ip destination** *ip-address* command.

- CSCsd77751

  Symptoms: A router may sends empty or blank syslog messages. For example, this situation may occur after the following error messages have been generated:

  ```
  %SYS-3-LOGGER_FLUSHING, %OIR-SP-STDBY-6-CONSOLE, %SYS-SP-STDBY-3-LOGGER_FLUSHED,
  %PFREDUN-SP-STDBY-6-ACTIVE ...
  ```

  Conditions: This symptom is observed on a Cisco 7600 series.

  Workaround: There is no workaround.

- CSCsd80632

  Symptoms: A change to the 64-bit high capacity (HC) input traffic counter of a main interface does not equal the sum of the changes for the HC input traffic counters of its subinterfaces.

  Conditions: This symptom is observed on a Cisco router that is configured for SNMP when the main interface is configured for Frame Relay.

  Workaround: There is no workaround.

- CSCsd81275

  Symptoms: When a standby supervisor engine or standby RP comes up, the following error message may be generated:

  ```
  %PFINIT-SP-1-CONFIG_SYNC_FAIL: Sync'ing the private configuration to the standby
  Router FAILED, the file may be already locked by a command like: show config.
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for ISSU.

  Workaround: There is no workaround.

- CSCsd81407

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsd88401

  Symptoms: Incoming packets may be dropped at the GE-WAN port 2 on an OSM-2+4GE-WAN+. In addition, the output of the **show platform hardware gt48520 counters** command shows that "mac_rx_error" errors for the OSM-2+4GE-WAN+ are increasing.

  Conditions: This symptom is observed on a Cisco 7600 series that processes IPv4 TCP and UDP packets with a random data pattern on an OSM-2+4GE-WAN+ with hardware revision 2.4 or lower. Note that the symptom occurs only on GE-WAN port 2, not on the other ports.

Workaround: There is no workaround.

Further Problem Description: Both upgrade the Cisco IOS software image to an image that integrates the fix for caveat CSCsd88401 and change the hardware revision of the OSM-2+4GE-WAN+ to 2.5.

- CSCsd88636

  Symptoms: Continuous CPUHOGs may occur during the "ATM OAM Input" process, locking the console for a long time.

  Conditions: This symptom is observed on the MSFC of a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA and that has an ATM interface with several VCs that are configured for Single Cell Relay (VC Mode). These VCs are configured on a PA-A3-OC3 or PA-A6-OC3 port adapter that is installed in an enhanced FlexWAN module. The symptom occurs after the peer router that is connected to the ATM interface (and on which the PVPs are configured) is reloaded.

  Note that the symptom is not platform- or release-dependent.

  Workaround: When the console is less busy, shut down the ATM interface on the peer router. The CPUHOGs may stop after some time. If this is not an option, there is no workaround.

- CSCsd94127

  Symptoms: An egress CoS is unexpectedly rewritten by the Internet Printing Protocol (IPP) on the ingress side.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when multicast traffic is routed over an ingress trunk interface on which the **mls qos trust cos** interface configuration command is enabled.

  Note that the symptom occurs only for routed multicast traffic. The symptom does not occur for other traffic such as layer 2 multicast and layer 2/layer 3 unicast traffic.

  Workaround: There is no workaround.

- 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.

- CSCsd95575

  Symptoms: A switch or router crashes because of a TEMPALARM message on the SP.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have a Supervisor Engine 720 router and occurs only with an automated script, often when the script runs the **clear ip route *** command.

  Workaround: There is no workaround.

- CSCsd98390

  Symptoms: A WS-X6148A-45AF module may not boot when you power-cycle the platform. The output of the **show module** shows the module status as "unknown." In addition, one or more modules may lose their configuration.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with eight or more modules.

  Workaround: Do not power-cycle the platform but enter the **reload** command.

- CSCse12154

  Symptoms: A router may crash because of a bus error when you enter the **copy scp** command to copy a configuration.

  Conditions: This symptom is observed on a Cisco router that is configured for SSH.

  Workaround: Do not use SCP. Rather, use Remote Copy Protocol (RCP) or use a TFTP transfer.

- CSCse24889

  Symptoms: Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

  Conditions: This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

  Workaround: As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

  ```
  config t
  ip ssh version 1 end
  ```

  Alternate Workaround: Permit only known trusted hosts and/or networks to connect to the router by creating a vty access list, as in the following example:

  ```
  10.1.1.0/24 is a trusted network that
  is permitted access to the router, all
  other access is denied

  access-list 99 permit 10.1.1.0 0.0.0.255
  access-list 99 deny any

  line vty 0 4
  access-class 99 in
  end
  ```

  Further Problem Description:

  For information about configuring vty access lists, see the Controlling Access to a Virtual Terminal Line document:

  http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cntrl_acc_vtl_ps6441_TSD_Products_Configuration_Guide_Chapter.html

  For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document:

  http://www.cisco.com/warp/public/707/ssh.shtml

- CSCse37587

  Symptoms: When DHCP snooping is enabled in conjunction with VRF, DHCP clients do not receive a DHCP IP address.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that function as a DHCP server.

  Workaround: There is no workaround.

- CSCse40423

  Symptoms: A tunnel interface cannot ping the other end of an IP tunnel.

  Conditions: This symptom is observed when ATM is configured and when the tunnel interface is up.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the tunnel interface.

- CSCse49388

  Symptoms: On a physical interface or subinterface on which a tunnel is configured and that encrypts or decrypts traffic, when you shut down and bring up the physical interface or subinterface multiple times, MAC entries for all VLANs that support the tunnel may be removed.

  When this situation occurs, when the “RMac reference” counter reaches 1, and when you shut down the physical interface or subinterface for the last time, packets are prevented from traversing the tunnel.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with either a Supervisor Engine 32 or a Supervisor Engine 720 and with a SIP-400 in which an IPsec VPN SPA is installed.

  Workaround: To prevent the symptom from occurring, do not shut down and bring up the physical interface or subinterface that supports the IPsec tunnel. When the symptom has occurred, reload the SIP-400 to reset the “RMac reference” counter to the original value.

  Further Problem Description: To see if the symptom has occurred, check the “RMac reference” counter as follows:

  ```
  # remote login switch
  sp# test mls net debug task 1 stat
  ...
  Netflow RMac List:
  0013.5f21.9100[14] <<-- where [n] is the reference count, in this case 14.
  Tunnel Interface(s):
  ...
  sp#
  ```

  You can check the counter each time after you have shut down and brought up the physical interface or subinterface. If, after every iteration, the reference count keeps decrementing towards 0, it means the symptom has occurred. A flapping link does not cause this problem. The “RMac reference” counter decreases each time that you shut down the physical interface or subinterface, perform and OIR of the SPA, or reset the SPA.

- CSCse56501

  A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

  Cisco is providing fixed software to address this issue. 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-20080326-IPv4IPv6.shtml.

- CSCse56921

  Symptoms: A platform that is configured for GPRS Tunneling Protocol (GTP) Server Load Balancing (SLB) may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when the same International Mobile Subscriber Identity (IMSI) is sent in two or more Packet Data Protocol (PDP) requests to different virtual servers and occurs when the sticky table entries time-out.

Workaround: There is no workaround.

- CSCse69713

  Symptoms: When all cache engines in a WCCP service group are inactive, the traffic is handled by the software; the traffic is CEF-switched by the software instead of FIB-switched in the hardware.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: Remove and re-enter the **ip wccp webcache** command.

- CSCse97422

  Symptoms: When you enter the **show tech** command with long a regular expression, the platform may crash during the display of the command output. For example, this situation may occur when you enter the following command:

  ```
  show tech |  e (0.00%  0.00%  0.00%|cmd_sts|0  0|ast clearing|packets input|packets
  output|SESs|LMI enq|cast queue|Last input|OAM cells input|reliability 255)
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with a Supervisor Engine 720.

  Workaround: Do not use a long regular expression when you enter the **show tech** command.

- CSCsf03566

  Symptoms: On a router that functions as an EzVPN server, a software-forced crash may occur because of memory corruption.

  Conditions: This symptom is observed on a Cisco 7600 series router that runs Cisco IOS Release 12.2(18)SXF when Extended Authentication (Xauth) is enabled while the crypto session is brought down. The symptom is both platform- and release-independent.

  Workaround: There is no workaround.

- CSCsf07232

  Symptoms: Tcl standard I/O operations such as a **puts** command may not display text on the terminal line under which the Tcl code is running. The text may be displayed on the terminal line that was the first one to connect (for example, vty0) or may not be displayed anywhere. Both print to standard output (STDOUT) and standard error (STDERR) streams are affected.

  Conditions: This symptom is observed on a Cisco router when more than one user is logged into a device, when one user enters Tcl Shell mode via the **tclsh** command, and then a second user enters Tcl Shell mode.

  Workaround: Ensure that only one user is connected to the device when Tcl standard I/O operations are run. If this is not an option, there is no workaround.

  Further Problem Description: When Tcl standard I/O operations are run on vty0 with only one user logged in, the text is displayed correctly.

- CSCsf12082

  Certain Cisco Catalyst 6500 Series and Cisco 7600 Router devices that run branches of Cisco IOS based on 12.2 can be vulnerable to a denial of service vulnerability that can prevent any traffic from entering an affected interface. For a device to be vulnerable, it must be configured for Open Shortest Path First (OSPF) Sham-Link and Multi Protocol Label Switching (MPLS) Virtual Private Networking (VPN). This vulnerability only affects Cisco Catalyst 6500 Series or Catalyst 7600 Series devices with the Supervisor Engine 32 (Sup32), Supervisor Engine 720 (Sup720) or Route Switch Processor 720 (RSP720) modules. The Supervisor 32, Supervisor 720, Supervisor 720-3B, Supervisor 720-3BXL, Route Switch Processor 720, Route Switch Processor 720-3C, and Route Switch Processor 720-3CXL are all potentially vulnerable.

OSPF and MPLS VPNs are not enabled by default.

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

- CSCsf14994

  Symptoms: A ping may not go through an MLP interface that is configured on a channelized T1/E1 SPA, channelized T3 SPA, or channelized STM-1 SPA.

  Conditions: This symptom is observed on a Cisco 7600 series when the following sequence of events occurs:

  1. You remove a multilink interface by entering the **no interface multilink** *multilink-bundle-number* command without first removing the member links from the bundle.
  2. You recreate the same multilink interface.
  3. You configure the multilink bundle by adding links from a different SPA that is installed in the same SIP.

  Workaround: First remove the **multilink-group** command from the member link configuration before you enter the **no interface multilink** *multilink-bundle-number* command.

- CSCsf31458

  Symptoms: The entPhysicalIndex object of the ENTITY-MIB may not remain the same after an SSO switchover has occurred on a Supervisor Engine 32.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series.

  Workaround: There is no workaround.

- CSCsf97682

  Symptoms: An E3/T3 interface that is located on a SPA in a SIP-200 does not come up. The controller is active, but the line-protocol remains down. Even with a physical loop, the E3/T3 interface does not enter the UP/UP (looped) state.

  Conditions: This symptom is observed on a Cisco 7600 series that has a SUP720-3BXL supervisor engine that runs Cisco IOS Release 12.2(33)SRA2 or Release 12.2(33)SRA3. For the symptom to occur, the diagnostics must be minimal or complete.

  Workaround: Configure bypass for the diagnostics by entering the **diagnostic bootup level bypass** command. Then, reset the SIP-200 by entering the **hw-module module** *slot-number* **reset** command or reload the SPA by entering the **hw-module subslot** *slot/subslot* **reload** command.

  Further Problem Description: The symptom does not occur in Release 12.2(33)SRB and Release 12.2(33)SRA1.

- CSCsf98345

  Symptoms: An MPLS LDP peer on a default VRF resets when a VRF interface goes down.

  Conditions: This symptom is observed on a Cisco router when the VRF interface is configured with a subnetwork address that overlaps with the default router ID.

  Workaround: Reconfigure the VRF interface address so it does not overlap with the default router ID.

- CSCsg02241

  Symptoms: Incorrect NAT translation may occur for one or more faulty Multilayer Switching (MLS) flows. You can recognize a faulty MLS flow in the output of the **show mls netflow ip** command. If any two MLS flows show the same adjacency, one of the MLS flows is faulty.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for NAT and occurs regardless of whether or not a Supervisor Engine 32 or Supervisor Engine 720 is configured for central or distributed forwarding.

Workaround: There is no workaround. Note that the symptom does not occur in Release 12.2(18)SXF8 and later releases.

- CSCsg02605

  Symptoms: After a packet buffer parity error has occurred on one port of a group of 12 ports, an Ethernet module does not go through the rapid reboot process but rather reboots regularly, which takes about 40 seconds.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router and affects the following modules when these are configured for to reset as a corrective action after an error has occurred:

  - WS-X6348-RJ-45
  - WS-X6348-RJ-21V
  - WS-X6248-RJ-45
  - WS-X6248-TEL
  - WS-X6148-RJ-45
  - WS-X6148-RJ-21

  Workaround: There is no workaround.

- CSCsg03483

  Symptoms: When you attempt to create a new VRF, the following error message may be generated:

  ```
  %FIB-SP-STDBY-4-FIBCBLK: Missing cef table for tableid 2 during route update XDR event
  SLOT 2:
  %FIB-4-FIBCBLK: Missing cef table for tableid 2 during route update XDR event
  %FIB-SP-4-FIBCBLK: Missing cef table for tableid 2 during route update XDR event
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA1 but may be platform- and release-independent.

  Workaround: There is no workaround.

- CSCsg03739

  Symptoms: A memory leak may occur in the “Crypto IKMP” process.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with an IPSec VPN SPA (SPA-IPSEC-2G).

  Workaround: There is no workaround.

- CSCsg08200

  Symptoms: The bootup diagnostics for a line card may detect a major failure after an RPR switchover has occurred, and these line cards reset repeatedly and eventually power-down.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router and occurs only with a Supervisor Engine 720 that is configured with a PFC3BXL (WS-SUP720-3BXL) or with a DFC3BXL-equipped module.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur after an SSO or RPR+ switchover has occurred.

- CSCsg10075

  Symptoms: When you enter the **show policy-map interface** command, the platform may hang at the --More-- prompt.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router but may also affect other platforms.

  Workaround: There is no workaround.

- CSCsg16425

  Symptoms: The output of the **show ip slb reals** command displays very large connection values (conns) for some real servers.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for Cisco IOS Server Load Balancing (IOS SLB) with inter-firewall routing enabled via the **ip slb route inter-firewall** command. The symptom occurs only when the inter-firewall connections switch from one firewall real to other firewall real in the firewall farm.

  Workaround: Remove and reconfigure the real server that is part of the server farm or firewall farm.

  Further Problem Description: When the connection value for a real server becomes very large, the server may enter the "MAXCONNS" state. When this situation occurs, you can no longer clear the connections counter by entering the **clear ip slb counters** or **clear ip slb connections** command.

- CSCsg19208

  Symptoms: When you reload a PE router, the standby RP crashes.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router in an MPLS configuration with TE tunnels and per-VRF-aggregate labels.

  Workaround: There is no workaround.

- CSCsg21429

  Symptoms: The interface of an OSM-1OC48-POS-SI+ module may flap after you have entered the **redundancy force-switchover** command.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with redundant Supervisor Engine 720-3BXL modules that function in RPR+ mode.

  Workaround: Repeat the **redundancy force-switchover** command several times.

- CSCsg24609

  Symptoms: A MIB walk on the CISCO-L2-CONTROL-MIB occurs very slowly.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that do not have the **mac-address-table limit vlan** *vlan* command enabled.

  Workaround: Enter the **mac-address-table limit vlan** *vlan* command.

- CSCsg35506

  Symptoms: After a Gigabit Ethernet (GE) interface has flapped, a mismatch may occur on a port channel, preventing the GE interface from joining the port channel. This situation occurs when the default flow control operational mode on the GE interface is unexpectedly changed from "off/off" to "on" after the GE interface has flapped.

  If the symptom occurs for the first interface of a group of interfaces that is supposed to join the port channel, none of the interfaces in the group can join the port channel, degrading the bandwidth and possibly causing severe packet drops on the channel.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router, and affects the following modules:

- Supervisor Engines 1 and 1a
- Supervisor Engine 2
- WS-X6408-GBIC
- WS-X6416-GBIC
- WS-X6516-GBIC and WS-X6516A-GBIC

Note that the symptom does not occur with the WS-X6724-SFP and the WS-X6748-GE-TX.

Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected GE interface.

Further Problem Description:

- Any operation that causes flow control negotiation triggers the symptom. For example. problem, entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command, resetting the module, performing an OIR, an RPR switchover, and so on.
- The symptom tends to occur when many ports are brought up simultaneously.

- CSCsg37484

  Symptoms: A router may reload because of a bus error in a crypto map and generate the following error message:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x4284A878
  ```

  Conditions: This symptom is observed on a Cisco router that has an IPSec crypto map.

  Workaround: There is no workaround.

- CSCsg40425

  Symptoms: An Optical Services Module (OSM) may reset unexpectedly and generate the following error messages:

  ```
  %POSLC-3-SOP: TxSOP-0 SOP. (source=0x18, halt_minor0=0x4000)
  %CWANLC-3-FATAL: Fatal Management interrupt, gen_mgmt_intr_status 0x0,
  line_mgmt_intr_status 0x1, reloading
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series.

  Workaround: There is no workaround.

- CSCsg40567

  Symptoms: Malformed SSL packets may cause a router to leak multiple memory blocks.

  Conditions: This symptom is observed on a Cisco router that has the **ip http secure server** command enabled.

  Workaround: Disable the **ip http secure server** command.

- CSCsg42246

  Symptoms: High CPU use may occur in the “IP Background” process, and the router may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router that is configured for RIP and that receives a RIP host route that is subsequently replaced by a route that is dynamically assigned to an interface. For example, this situation may occur on a PPP interface that has the **ip address negotiated** command enabled.

Workaround: Use a route map to block the advertised route.

- CSCsg43284

  Symptoms: A VPN tunnel may fail to establish a proper connection to a Cisco Catalyst 6500 series switch or Cisco 7600 series router because fragmented ISAKMP packet are dropped by the IPSec VPN Services Module (SPA-IPSEC-2G).

  Conditions: This symptom may occur for many reasons, including the following:

  - The peer sends too many different proposals.
  - The certificate that is used by the peer is too large, for example, because the key is too large, the issuer-name is long, the subject-name is long, the are many CDPs, and so on.

  Workaround: In some circumstances, when the peer is an EzVPN client router that runs Cisco IOS Release 12.4T, changing the Cisco IOS software image to Release 12.4 may reduce the size of the proposals.

  When the certificate of the peer is too large, reduce the size of the RSA key, and/or remove or reduce long fields in the certificate.

  Further Problem Description: When the symptom occurs, a packet capture of all traffic that is received by and sent to the switch or router shows the following:

  - The fragmented ISAKMP packets that are sent to the switch or router.
  - The response (several seconds or up to one minute later) of the switch or router with the following ICMP packet:

    ```
    Type: 11 (Time-to-live exceeded)
    Code: 1 (Fragment reassembly time exceeded)
    ```

- CSCsg47462

  Symptoms: A router that is configured with at least one multipoint GRE tunnel may crash with an address error.

  Conditions: This symptom is observed when a T3 interface bounces while the CPU usage of the router is at 100 percent.

  Workaround: There is no workaround.

- CSCsg61773

  Symptoms: Egress multicast forwarding may not function when an outgoing interface (OIF) flaps very quickly.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when Multicast MultiLayer Switching (MMLS) is configured (MMLS is configured by default).

  Workaround: There is no workaround.

  Further Problem Description: When an interface flaps very quickly, the module mask may not be allocated for the interface, causing the egress multicast functionality to be affected. In this situation, the interface may not function properly as an OIF.

- CSCsg69646

  Symptoms: An IPSec VPN SPA (SPA-IPSEC-2G) may stop forwarding traffic over GRE tunnels that are configured with tunnel protection.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router and occurs on a rare intermittent basis when the CPU processing load of the RP is high, for example, when there is a large number of crypto certificates being processed.

Workaround: There is no workaround.

- CSCsg73179

  Symptoms: After a change in the routing topology, a Bidirectional PIM Rendezvous Point is not updated correctly in the hardware tables, causing Bidirectional PIM multicast flows to be software-switched.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router and occurs only when the ACL that is used to statically configure the Rendezvous Point does not have any wildcard entries.

  Workaround: Reinstall the Rendezvous Point.

- CSCsg79810

  Symptoms: The MPLS MTU is overruled by the IP MTU on an ATM interface.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in an MPLS core when the ATM interface has the **tag-switching mtu 1508** command and the **ip mtu 1500** command enabled. In this situation, packets that are larger than 1496 bytes are dropped.

  Workaround: There is no workaround.

- CSCsg90190

  Symptoms: Without the enforcement of a voice daughterboard connector rating, the number of IP phones that can be powered up may exceed the number that the voice daughterboard can handle, that is, the available allocated inline power can exceed the VDB connector rating.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsg99914

  Symptoms: A SIP-200 may reset unexpectedly because of a keepalive failure when there is a lot of IPC backplane traffic and when Ethernet Out of Band Channel (EOBC) traffic drops occur because of a low queue size at the EOBC level.

  Conditions: This symptom is observed on a Cisco 7600 series that functions with a scaled configuration when a major and sudden topology change causes many IPC messages on the backplane.

  Workaround: There is no workaround.

- CSCsh01749

  Symptoms: The **mls qos marking ignore port-trust** command may not function.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch or Cisco 7600 series router that has a Supervisor Engine 32 or Supervisor Engine 720. When you enter the **mls qos marking ignore port-trust** command for an interface that is configured with several subinterfaces, each with a service policy, the service policies are supposed to match a unique ingress CoS value and change the corresponding egress MPLS EXP value for transfer across an MPLS cloud. However, after you have entered the **mls qos marking ignore port-trust** command, all egress EXP values show up as 0 because the command has no effect.

  Workaround: There is no workaround.

- CSCsh07037

  Symptoms: A "%SYS-2- CHUNKBADMAGIC" error mat occur on an OSM module and the module may restart.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when Weighted Random Early Detection (WRED) is configured with a maximum threshold of more than 2000 packets but without a queue limit.

Workaround: Configure a proper queue limit for the class with the WRED configuration. For example, when the **random-detect precedence 3 32000 32000 1** command is configured, configure the queue limit by entering the **queue-limit 32768** command.

- CSCsh11498

  Symptoms: When you boot a switch or router with two SPA-IPSEC-2G SPAs in the same Services SPA Carrier (7600-SSC-400), one of the SPAs does not come up. When you attempt to boot the switch or router again, both SPAs come up properly.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsh13947

  Symptoms: A router that is processing certain MPLS forwarding updates may crash or hang because of a software configuration mismatch.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB but may also occur in other releases. The symptom occurs when EoMPLS or AToM is configured with many virtual circuits (VCs) and when LDP sessions go down because of extreme traffic loads or clearing of the LDP neighbors, causing the forwarding information to be modified.

  Workaround: There is no workaround.

- CSCsh17979

  Symptoms: When inline power ports can not be powered on, a command may be rejected with the following error message:

  ```
  Command rejected: there's not enough system power to be allocated to Fa1/47, or the
  maximum power the backplane of this chassis can support has reached the limit.
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with a module with a voice daughtercard.

  Workaround: There is no workaround.

- CSCsh20354

  Symptom 1: A third-party vendor VPN client may not be able to establish a VPN tunnel to a Cisco router. When you enable the **debug crypto isakmp** command on the Cisco router, the output shows the following:

  ```
  ISAKMP:(0:4:HW:2):No IP address pool defined for ISAKMP!
  ISAKMP:(0:4:HW:2):deleting SA reason "Fail to allocate ip address" state (R)
  CONF_ADDR     (peer x.x.x.x)
  ```

  Symptom 2: Although a third-party vendor VPN client can establish a VPN tunnel to a Cisco router, the client receives only an IP address but no DNS configuration, split-tunnel information, or other data during the mode configuration phase. In this situation, the debug output does not show any errors.

  Conditions: Both of these symptoms are observed only when a third-party vendor VPN client connects to a Cisco router that functions as a VPN server.

  Workaround: There are no workarounds.

- CSCsh22835

  Symptoms: After an RPR switchover occurs, a major error occurs on the newly active RP.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

Workaround: Reload the platform. If this not an option, there is no workaround.

- CSCsh23981

  Symptoms: During an HA switchover while IPC traffic is sent between the standby RP and standby SP, the newly active RP may crash.

  Conditions: This symptom is observed on Cisco Catalyst 6000 series switches and Cisco 7600 series routers. For Cisco Catalyst 6000 series switches, the symptom occurs in Release 12.2SX and Release 12.2SXF, in which ISSU is not supported. For Cisco 7600 series router, the symptom occurs in Release 12.2(33)SRB, in which ISSU is supported.

  Workaround: There is no workaround.

- CSCsh29863

  Symptoms: On an RPR switchover, the new active crashes during bootup diagnostics.

  Conditions: This symptom occurs when bad SFPs are plugged into the SFP- capable ports. Bad SFP means incompatible/unsupported/faulty SFP.

  Workaround: Remove incompatible/unsupported/faulty SFPs from the SFP port(s) and plug in a good one if needed.

- CSCsh31287

  Symptoms: The source MAC address for multicast on a tunnel that is accelerated by a crypto engine may remain zero.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with an IPSec VPN Services Module (SPA-IPSEC-2G).

  Workaround: There is no workaround.

- CSCsh31306

  Symptoms: Output drops occurs on a T1 serial interface. These drops are shown in the output of the **show interface serial** command but are not shown at the QoS level, that is, the output of the **show policy-map interface** command does not indicate any drops.

  When this situation occurs, the output of the **show controller** command for the serial interface at the VIP or FlexWAN level shows “pascb.tx_polling_high” with any value other than 2.

  Conditions: The symptoms is observed on a Cisco 7500 series (with a VIP) and Cisco 7600 series (with a FlexWAN module) that have a serial interface that is configured for fair-queueing.

  Workaround: Remove and then reconfigure fair-queueing so that “pascb.tx_polling_high” is set to the correct value of 2.

- CSCsh33770

  Symptoms: An IPSec VPN SPA (SPA-IPSEC-2G) may not come up during the boot process, that is, it remains in the “Initializing” state. The output of the **show crypto eli** command shows the following information:

```
Hardware Encryption : INACTIVE
Number of hardware crypto engines = 1

CryptoEngine SPA-IPSEC-2G[6/0] details: state = Initializing
Capability      :
IPSEC: DES, 3DES, AES, RSA

IKE-Session   :     0 active, 16383 max, 0 failed
DH            :     0 active,  9999 max, 0 failed
IPSec-Session  :      0 active, 65534 max, 0 failed
```

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that run Cisco IOS Release 12.2SRA.

Workaround: There is no workaround.

- CSCsh51688

  Symptoms: A Cisco 7600 series may crash unexpectedly because of a bus error on the Switch Processor (SP). The following error message may be generated prior to the crash:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x40B450D4
  ```

  Conditions: This symptom is observed on a Cisco 7600 series and the trigger is currently not known.

  Workaround: There is no workaround.

- CSCsh54325

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

  Symptom 1: When frames require PXF punting to the RP (or SP), PPP LCP frames may not be forwarded to the RP (or SP), causing link negotiation to fail. Or, HDLC keepalives may not be forwarded to the RP (or SP), causing the link to remain down.

  Condition 1: These symptoms are observed on a Cisco Catalyst 6503, Cisco Catalyst 6503-E, and Cisco 7604 that are configured with a SIP-600 in which a POS SPA is installed and occurs when the supervisor engine resides in slot 1 or slot 2 of the chassis.

  Workaround 1: There is no workaround.

  Symptom 2: When frames require PXF punting to the RP (or SP), CFM PDUs may not be properly forwarded to the RP (or RP).

  Condition 2: This symptom is observed on a Cisco 7604 that is configured with a SIP-600 or Ethernet Services line card (ES20) and occurs when the supervisor engine resides in slot 1 or slot 2 of the chassis.

  Workaround 2: There is no workaround.

- CSCsh56121

  Symptoms: After you have reloaded a Cisco 7600 series that has redundant supervisor engines, or after you have forced a redundancy switchover, the RSA key on the standby supervisor engine may be lost.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA2.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reconfigure the RSA key.

- CSCsh61946

  Symptoms: After an SSO switchover has occurred, the second of two 6000 W DC power supplies in the chassis is shut down.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 router when both power supplies are powered on before the SSO switchover occurs.

  Workaround: There is no workaround.

- CSCsh65322

  Symptoms: A Cisco 7600 series with an Enhanced FlexWAN in which a PA-A3-OC3SMI port adapter is installed may drop packets steadily from the ATM interface. This situation may be verified under the “Total output drops” in the output of the **show interfaces atm** command.

Conditions: This symptom is observed when the router is configured for PPPoA connections. There is no correlation between the packet drops on the interface and any particular ATM PVCs or virtual-access interfaces. The symptom may also occur on other platforms that are configured with a PA-A3-OC3SMI port adapter.

Workaround: There is no workaround.

Further Problem Description: note that the symptom does not occur with a FlexWAN.

- CSCsh76923

  Symptoms: A Cisco Catalyst 6500 series switch may crash because of memory corruption or a bus error.

  Conditions: This symptom is observed when NAT is configured. The symptom may also affect a Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsh83559

  Symptoms: A Cisco Catalyst 6000 series switch may leak memory in the IP Input task in the Cisco IOS-BASE process. The memory is leaked in a small amount per packet that is process switched over a VRF on the switch. Non-VRF traffic is not affected.

  Conditions: This symptom is seen on a Cisco Catalyst 6000 series switch that is running Cisco IOS Modularity. This can only happen if there are VRFs configured on the switch.

  Workaround: Do not use VRFs.

- CSCsh94940

  Symptoms: An active supervisor engine may crash because of memory corruption in the SP processor pool, and the following error message may be generated:

  ```
  %SYS-SP-3-BADFREEMAGIC: Corrupt free block at [...] (magic [...])
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with a Supervisor Engine 32 when a periodic SNMP query is made to the L2 MAC table. Because of a race condition, freed memory may be written by another thread, causing memory corruption.

  Note that the symptom does not occur with a Supervisor Engine 1 and Supervisor Engine 2.

  Workaround: Disable the SNMP query to the L2 MAC table.

- CSCsi01151

  Symptoms: When IPSec SA rekeys, an SPI deletion error may occur, causing one peer to use the outbound SA that has been deleted by the other peer.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with an IPSec VPN Services Module (SPA-IPSEC-2G). The symptom occurs when both the Cisco platform and its peer rekey at the same time, preventing the Cisco platform from deleting the old SPI, causing multiple SPIs to be generated on the Cisco platform, and causing the Cisco platform to use the wrong SPI to encrypt the packets.

  Workaround: Clear the tunnel.

- CSCsi01422

  Symptoms: Frame Relay traffic shaping in a configuration with a child policy and hierarchical QoS does not function. Traffic does not respond to BECN or FECN marking.

  Conditions: This symptom is observed on a Cisco 7600 series when a service policy is configured under a Frame Relay map class. Note that the symptom is platform-independent.

Workaround: There is no workaround.

- 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.

- CSCsi02033

  Symptoms: On a PE router, a subinterface on which an EoMPLS VC is configured may stop forwarding traffic from the backbone to a CE router. Traffic that is sent from the PE router to the CE router goes through fine. Traffic forwarding from the backbone is affected.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA3 or an earlier release and that functions as a PE router. The symptom occurs when you configure a new subinterface and an IP address on a Gigabit Ethernet (GE) interface that is installed in a SIP-400 and that connects to a remote CE router. In this situation, another subinterface (on the same GE interface) that is configured for EoMPLS no longer functions for traffic that is forwarded from the backbone to the CE router.

  Workaround: Remove and reconfigure Xconnect on the affected subinterface.

  Alternate Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the physical interface on which the affected subinterface is configured.

- CSCsi02778

  Symptoms: When the MPLS Traffic Engineering (TE)-Fast Reroute (FRR) Link and Node Protection feature is enabled, VPLS traffic does not flow from end-to-end after it has been rerouted to single-hop backup tunnel.

  Conditions: This symptom is observed on a Cisco 7600 series when the primary tunnel is a multihop tunnel with implicit-null as the next-hop label and when the backup tunnel is single-hop tunnel. After traffic has been rerouted to the backup tunnel, VCs do come up and the egress path for VPLS VCs is shown correctly as the backup tunnel. However, the traffic does not reach the egress PE router.

  Workaround: There is no workaround.

  Further Problem Description: From the egress line card, enter the following **show** commands to collect information to further debug this issue:

  – Enter the **show platform atom ether-vc** command to identify the egress index of the VPLS VC.

  – Enter the **show platform mpls imposition-table details** command to look at the egress information.

  After traffic has been rerouted to the backup tunnel, the egress label operation is incorrectly programmed to forward the original primary TE label on the label stack.

- CSCsi06759

  Symptoms: When you run the **snmpwalk** command, the ifIndex for the subinterfaces of a SIP-200 is not retrieved although the output of a **show** command does show the ifIndex. When you run the **snmpwalk** command, the following error message and a possible traceback are generated:

  ```
  %SNMP-3-DVR_DUP_REGN_ERR: Attempt for dupe regn with SNMP IM by driver having ifIndex
  <index> and ifDescr <description>
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router after you have replaced a FlexWAN module with a SIP-200.

  Workaround: There is no workaround.

- CSCsi10219

  Symptoms: A SIP-200 may crash, and a SIP heartbeat failure message may be generated on the console of the RP.

  Conditions: This symptom is observed on a Cisco 7600 series that has a SIP-200 that is configured for hardware-based MLP and cRTP and in which a SPA-8XCHT1/E1, SPA-1XCHSTM1/OC3, SPA-2XCT3/DS0, or SPA-4XCT3/DS0 is installed. The symptom occurs when RTP traffic is processed on the MLP bundle.

  Workaround: Do not configure hardware-based MLP. Rather, when cRTP is required, configure software-based MLP.

- CSCsi14145

  Symptoms: The runt counter is updated with runt frames with CRC errors while runt frames with proper CRCs are ignored.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when packets with a size smaller than 64 bytes are received. The output of the **show interface** command accounts only for packets as runt frames that are smaller than 64 bytes and that have CRC errors. Thus, statistics are lost.

  Workaround: There is no workaround.

  Further Problem Description: According to the 802.3 specifics and information on the IEEE website, the definition of runt frames is:

  Runts: Frames that are smaller than the minimum frame size for IEEE-802.3 standard frames. Runt frames typically are caused by collision fragments and are propagated through the network. If the number of runt frames exceeds the number of collisions, there is a problem with a transmitting device.

- CSCsi71285

  Symptoms: SNMP walk of VLAN statistics or executing the **show vlan counters** CLI command causes indefinite console wait or CPUHOG.

  Conditions: This defect is seen only in Cisco IOS Release 12.2SRA images.

  Workaround: VLAN statistics are collected from cached entries instead of collecting real time statistics, which was causing indefinite wait on IPC calls.

  Further Problem Description: Both SNMP queries and CLI commands will block while retrieving nonrouted VLAN counters. An SNMP query on any of the ifTable counters for a nonrouted VLAN interface will block the SNMP Agent indefinitely. This causes the SNMP AGENT queue to fill up and start dropping SNMP packets. This problem in turn prevents the Network Management application from accessing any other MIB objects not related to the nonrouted VLANs. Restarting the SNMP agent clears the thread, but as soon as another objects related to nonrouted VLAN is accessed, the SNMP agent will block again.

- CSCuk61773

  Symptoms: CPU spikes may occur on a router that is configured for Web Cache Communication Protocol (WCCP) earlier than Release 4.0.7.

  Conditions: This symptom is observed on a Cisco 7600 series when WCCP is in communication with a Cisco Wide Area Application Services (WAAS) appliance. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCek12203

  Symptoms: When you enter the **copy ftp disk** command, the copy operation may fail and cannot be terminated, further **copy** commands may fail, and a TCP vty session for the purpose of troubleshooting the situation may fail and cannot be terminated.

  Conditions: These symptoms are observed on a Cisco platform when the FIN flag is set in the initial ESTAB message from a neighbor. You must reload the router to recover from the symptoms.

  Workaround: Do not enter the **copy ftp disk** command. Rather, enter the **copy tftp disk** command.

- CSCsg39837

  Symptoms: HTTP errors may occur while accessing a Win2003 Web Server.

  Conditions: This symptom is observed on a voice gateway that runs Cisco IOS Release 12.4(6)T when a Win2003 HTTP web server is accessed under a heavy load and when the voice gateway has the **ip http client connection persistent** command disabled. Note that the symptom may also affect other releases.

  Workaround: There are two possible workarounds:

  1. Switch to a Win2000 HTTP web server.
  2. On a Win2003 server, set "TcpTimedWaitDelay" to the minimum (30 seconds). This does not totally eliminate but will reduce the occurrences of dropped TCP SYN requests from the Cisco IOS router.

Wide-Area Networking

- CSCek49202

  Symptoms: When an attempt to move an interface from one multilink group to another fails because of platform-specific limitations, the interface is left in an invalid state. The **multilink-group** command still appears in the interface configuration, but the interface does not appear in the output of **show ppp multilink** command.

  Conditions: This symptom may occur on platforms that support distributed implementations of multilink (such as the Cisco 7500 series, Cisco 7600 series, Cisco 10000 series, and Cisco 12000 series routers) when the platform does not allow the interface to be added to a multilink group for some reason, for example, because of resource constraints.

  Workaround: Enter the **no multilink-group** command to remove the interface from its current multilink group before adding it to a new one.

- CSCsd72854

  Symptoms: When IS-IS is configured on an MLP interface of a 6-port channelized T3 Engine 0 line card, the line card may fail to come up because PPP fails to negotiate OSICP on the MLP interface.

Conditions: This symptom is observed on a Cisco 12000 series router after you have reloaded the router. Note that the symptom may also occur on other platforms and in other releases.

Workaround: Increase the PPP timeout retry interval to 10 seconds by entering the **ppp timeout retry 10** command on the interface. (The default timeout retry interval is 2 seconds).

Resolved Caveats—Cisco IOS Release 12.2(33)SRA3

Cisco IOS Release 12.2(33)SRA3 is a rebuild release for Cisco IOS Release 12.2(33)SRA. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRA3 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsb89847

  Symptoms: Source and destination Border Gateway Protocol (BGP) autonomous system (AS) information may not be properly updated.

  Conditions: This symptom is observed on a Cisco router that is configured for MSDP and NetFlow.

  Workaround: There is no workaround.

- CSCse08044

  Symptoms: A Cisco router may generate export packets in which the first flow record contains incorrect data such as incorrect IP addresses.

  Conditions: This symptom is observed on a Cisco router that is configured for NetFlow and NetFlow Data Export.

  Workaround: Disable NetFlow.

- CSCsg48725

  Symptoms: A TLB exception may occur on a Cisco platform that functions as a PE router in an MPLS environment, and the following error message may be generated:

  ```
  TLB (load or instruction fetch) exception, CPU signal 10 (BadVaddr: DEADBEF3)
  ```

  Conditions: This symptom is observed on a Cisco platform when TACACs accounting and authorization is enabled and when the TACACs server is reachable through the global routing table.

  Workaround: Disable AAA. Is this not an option, there is no workaround.

Interfaces and Bridging

- CSCek43732

  Symptoms: All packets are dropped from a 1-port OC-3/STM-1 POS port adapter (PA-POS-1OC3) or 2-port OC-3/STM-1 POS port adapter (PA-POS-2OC3) that is configured for CBWFQ.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1. However, the symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCsd40136

  Symptoms: POS interfaces may remain in the up/down state after the router is upgraded to another Cisco IOS software image.

Conditions: This symptom has been observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router but may also affect other platforms such as the Cisco 7500 series router.

Workaround: Reload the FlexWAN or VIP in which the POS port adapter is installed.

IP Routing Protocols

- CSCsd15749

  Symptoms: Prefixes that are tagged with Site of Origin (SoO) values may not be filtered at the border.

  Conditions: This symptom is observed when SoO values are configured for a peer group. The peer group members may not correctly filter the prefixes that are based on the SoO value at the border.

  Workaround: BGP supports Dynamic Update peer groups, which ensure that packing is as efficient as possible for all neighbors regardless of whether or not they are peer-group members.

  Peer groups simplify configurations, but peer-templates provide a much more flexible solution to simplify the configuration than peer groups.

  If the SoO configuration is applied directly to the neighbor or to a template, the symptom does not occur. Using templates to simplify the configuration is a better solution and Dynamic Update peer groups ensure efficiency.

- CSCsd73245

  Symptoms: Many “IPRT-3-PATHIDX” error messages are generated by the “BGP Router” process when you increase the prefixes in a VRF.

  Conditions: This symptom is observed on a Cisco router that is configured for loadbalancing and that functions in an MPLS VPN environment.

  Workaround: There is no workaround.

- CSCsf20947

  Symptoms: A default route that is defined by the **neighbor default-originate** command may be ignored by the BGP neighbor.

  Conditions: This symptom is observed on a Cisco router after a route flap in the network causes the default route to be relearned.

  Workaround: Manually clear the BGP neighbor to enable the router to correctly relearn the default route.

- CSCsh61119

  Symptoms: ARP may be refreshed excessively on the default interface, causing high CPU usage in the “Collection Process.”

  Conditions: This symptom is observed on a Cisco router that has point-to-point interfaces that have non-/32 interface addresses or secondary addresses and that constantly come up or go down.

  Workaround: There is no workaround.

ISO CLNS

- CSCse40346

  Symptoms: Tracebacks may be generated when you configure IS-IS and LDP features, for example, when you enter the **no ip router isis** *area-tag* command.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(32)SY but may also occur in other releases.

Workaround: There is no workaround.

Miscellaneous

- CSCed36177

  Symptoms: A software-forced crash may occur on the RP in a Cisco Catalyst 6500 series switch or Cisco 7600 series router.

  Conditions: This symptom is observed only with a tunnel configuration and may occur with either crypto or non-crypto images.

  Workaround: There is no workaround.

- CSCek42751

  Symptoms: The running configuration may not be accessible after you have copied a small file to the running configuration.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system after you have rebooted the router.

  Workaround: Reboot the router once more.

- CSCek47814

  Symptoms: A ping between two CE routers may fail after you have reloaded the CE router on the Ethernet side.

  Conditions: This symptom is observed in an AToM configuration when one CE router is configured for PPP and the other CE router is configured for Ethernet. The symptom occurs because of a MAC address learning failure.

  Workaround: Reconfigure VLAN over MPLS on the corresponding Ethernet interface of the adjacent PE router.

- CSCek60775

  Symptoms: A router that has Virtual Tunnel Interfaces (VTIs) may crash.

  Conditions: This symptom is observed when two VTIs are configured with the same IP address and when the inside VRF (IVRF) of one VTI is the same as the Front Door VRF (FVRF) for the other VTI.

  Workaround: There is no workaround. The configuration that is stated in the Conditions is not considered a valid configuration.

- CSCek61974

  Symptoms: You may be able to configure a minimum receive interval as short as 1 ms, which may cause problems on the router.

  Conditions: This symptom is observed on a Cisco router that supports Bidirectional Forwarding Detection (BFD). Note that a minimum receive interval shorter than 50 ms is not supported in Cisco IOS software images.

  Workaround: Configure a minimum receive interval of 50 ms or longer.

- CSCek65022

  Symptoms: A 7600-SSC-400 may crash on bootup.

Conditions: This symptom is observed when the Cisco IPsec VPN Shared Port Adapter (SPA-IPSEC-2G) is booting up.

Workaround: There is no workaround.

- CSCek66294

  Symptoms: TCP MSS adjusts feature works only on the ingress direction. The feature should work on both ingress and egress directions.

  Conditions: This symptom has been observed when the TCP MSS adjusts feature is configured.

  Workaround: There is no workaround.

- CSCek68218

  Symptoms: A SIP-600 may crash when the **diagnostic bootup level** command is enabled.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a SIP-600 in which a 16-port Gigabit Ethernet GBIC (WS-X6516-GBIC) is installed.

  Workaround: Bypass the diagnostic test by entering the **no diagnostic bootup level** command.

- CSCin74155

  Symptoms: A router that functions under a heavy load with SSHv2 clients may crash if any of the SSH clients are terminated.

  Conditions: This symptom is observed when the following conditions are present:

  - The CPU utilization above 70 percent.
  - There are continuous sweep pings from two far-end routers that have the **debug ip packet** command enabled to create continuous logs for the SSH clients.
  - The **no logging console** command is configured.
  - A connection is made from a couple of SSHv2 clients, you enable the **terminal monitor** command, and you terminate the SSHv2 clients while continuous messages are being generated.
  - The TCP window size is reduced.

  Workaround: Avoid using SSHv2 when the router is very stressed.

- CSCsb89043

  Symptoms: The following error message and traceback are generated when an RP switchover occurs:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x603D9154 reading 0x4C
  -Traceback= 603D9154 603DA078 603DA0C0 603DA65C 603DA740 603DA8AC 603DA9AC 603C92F4
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for HA.

  Workaround: There is no workaround. However, the symptoms do not affect the performance of the router or the processing of traffic.

- CSCsc60249

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254

  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCsc72722

  Symptoms: TCP connections that are opened through a Cisco IOS Firewall (CBAC) may not timeout.

  Conditions: With Cisco IOS Firewall (CBAC) enabled, the TCP idle timer for a session may be reset even by TCP packets that fail TCP inspection and are subsequently dropped. This could lead to the TCP session not timing out.

  Workaround: There is no workaround.

- CSCsd29469

  Symptoms: SNMP polls hang at a specific point, after which there is no response for a long time. Then, SNMP polling works fine for a while until it hangs again at a specific point.

  When SNMP becomes unresponsive, the following error message may be generated, and SNMP queries may time-out at the application:

  ```
  %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full
  ```

  Conditions: These symptoms are observed under the following conditions:

  - After a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have a Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXF2 have been polled for a while.
  - After the CISCO-ENHANCED-MEMORY-POOL-MIB is polled on a Cisco 7600 series router that has a Supervisor Engine 720 that runs Cisco IOS Release 12.2(33)SRA.

  Workaround: Exclude the CISCO-ENHANCED-MEMORY-POOL-MIB from the SNMP view. Enter the following commands to exclude the CISCO-ENHANCED-MEMORY-POOL-MIB:

  ```
  snmp-server view public-view iso included
  snmp-server view public-view ciscoMemoryPoolMIB excluded
  snmp-server view public-view ciscoEnhancedMemPoolMIB excluded
  snmp-server community public view public-view RO
  ```

  This view should be applied to all community strings that might be used to poll these MIB modules. If views are already applied to a community string then the one above and the existing view should be merged.

  If SNMPv3 is in use then this view should be applied to any SNMPv3 groups configured as well.

  There is no need to reboot the platform. The symptom should resolve itself within a few minutes. If you must immediately clear the symptom, enter the following two commands (use one of the SNMP server community string commands that are actually configured on the router instead of the ones that are mentioned in the example below, which are based on the information that is presented above):

  Disable SNMP and stop the processes:

  ```
  no snmp-server
  ```

Re-enable SNMP and restore the SNMP configuration:

```
snmp-server community public view public-view RO
```

Further Problem Description: When you enable the **debug snmp packet** command, you can see that the SNMP poll requests are not being acknowledged. However, the output of the **show snmp counters** command shows about the same number of SNMP requests as the number of outputs, even though these outputs were never processed and sent.

- CSCsd40211

  Symptoms: After you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an interface, ARP may be delayed. After 5 to 30 minutes, ARP finally appears for the interface in the MAC address table of the switch processor.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(18)SXD4 or Release 12.2(18)SXE4 and that is configured for NetFlow. The symptom may also affect other releases such as Release 12.2SR.

  Workaround: There is no workaround.

- CSCsd85587

  A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  The vulnerable cryptographic library is used in the following Cisco products:

  - Cisco IOS, documented as Cisco bug ID CSCsd85587
  - Cisco IOS XR, documented as Cisco bug ID CSCsg41084
  - Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
  - Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
  - Cisco Firewall Service Module (FWSM)

  This vulnerability is also being tracked by CERT/CC as VU#754281.

  Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

Note Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

- CSCse09498

  Symptoms: When you enter the **no shutdown** interface configuration command on an auto-template interface during deployment, some tunnels may be in the up/down state, and the tunnel mode may be GRE instead of the configured tunnel mode of MPLS.

  Conditions: This symptom is observed on a Cisco router with about 70 primary MPLS TE tunnels. The symptom occurs when you first enter the **no interface auto-template** command, then you enter the **tunnel mode mpls traffic-eng** command, and finally you paste the template back.

  Workaround: Reload the router.

  Alternate Workaround: Create an automesh in the following sequence:

```
conf t
access-list 60 permit 10.0.7.3
access-list 60 permit 10.0.1.5
access-list 60 permit 10.0.2.6
access-list 60 permit 10.0.3.7
access-list 60 permit 10.0.5.1
access-list 60 permit 10.0.6.2
access-list 60 permit 10.0.8.12

interface Auto-Template1
ip unnumbered Loopback0
no ip directed-broadcast
tunnel destination access-list 60
tunnel mode mpls traffic-eng
.........
access-list 60 permit 10.0.7.3
access-list 60 permit 10.0.1.5
access-list 60 permit 10.0.2.6
access-list 60 permit 10.0.3.7
access-list 60 permit 10.0.5.1
access-list 60 permit 10.0.6.2
access-list 60 permit 10.0.8.12
```

- CSCse11794

  Symptoms: A SIP-200 or SIP-400 may crash when you configure 12,000 bridged VCs along with a service policy on an ATM SPA that is installed in the SIP.

  Conditions: This symptom is observed on a Cisco 7600 series.

  Workaround: There is no workaround. To prevent the symptom from occurring, do not configure more than 1000 bridged VCs when there is also a service policy.

- CSCse17175

  Symptoms: The line protocol may go down on some of the serial interfaces of a 1-port multichannel STM-1 single mode port adapter.

  Conditions: This symptom is observed on a Cisco router when the maximum number of channel groups (256) is configured on the port adapter.

  Workaround: There is no workaround.

- CSCse26682

  Symptoms: When you enter the **no ipv6 unicast-routing** command followed by the **ipv6 unicast-routing** command, prefixes may be missing from the IPv6 CEF table on a line card. This situation may cause traffic loss.

  Conditions: This symptom is observed on a Cisco 7600 series.

Workaround: Although you can enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command for every interface that is configured for IPv6, doing so is inefficient. It is more efficient and less disruptive to enter the **clear cef table ipv6** command.

- CSCse68138

  Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

  - Session Initiation Protocol (SIP)
  - Media Gateway Control Protocol (MGCP)
  - Signaling protocols H.323, H.254
  - Real-time Transport Protocol (RTP)
  - Facsimile reception

  Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

  There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml.

- CSCse83031

  Symptoms: A memory leak may occur when you remove an Xconnect configuration from a router, which can be verified by enabling the **show memory debug** command.

  Conditions: This symptom is observed when you configure Xconnect with the Exchange Fabric Protocol (EFP) and then remove the Xconnect configuration.

  Workaround: There is no workaround.

- CSCse84226

  Symptoms: When a VC is down, the output of the **show connection** command on the local side shows that the VC is up, even though the output of the **show mpls l2 vc detail** command shows that the VC is down. The output of the **show connection** command on the remote side shows that the VC is down.

  Conditions: This symptom is observed on a Cisco router that is configured for AToM when the MTU mismatches the Virtual Private Wire Service (VPWS) circuit.

  Workaround: There is no workaround.

- CSCse90586

  Symptoms: A Cisco 7600 series that has a large number of OSPF tunnels with VRFs may run out of memory, many MALLOC failures may occur, and the router may reload because of a “Corrupted Program Counter” error. The crash traceback that is generated is invalid.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA, that is configured for OSPF, and that has 500 tunnels with a VRF configuration.

  Workaround: Reduce the number of tunnels and VRFs in the configuration.

- CSCsf19418

  Symptoms: A router may reload unexpectedly when you enter the **show mpls ldp graceful-restart** command.

  Conditions: This symptom is observed when either of the following conditions are present:

  – When the command output has a “Down Neighbor Database” entry that expires by reaching the reconnect timeout limit while the command output is generating the neighbor address list.

  – When the command output is paged at the “--More--” string within the context of displaying addresses.

  Workaround: Do not enter the **show mpls ldp graceful-restart** command when a graceful-restart database entry is about to expire. When the command output is paged at the “--More--” string within the context of displaying addresses and when the Down Neighbor Database entry may have expired, type the letter “Q” to abort any further output of addresses.

- CSCsg02554

  Symptoms: On a Cisco Catalyst 6500 series or Cisco 7600 series router that has two Optical Services Modules (OSMs) that are configured for APS, a switchover to the protect channel may result in a 30-second traffic loss.

  Conditions: This symptom is observed when the L2 protocol is configured for Frame Relay.

  Workaround: Disable keepalive on the Frame Relay link, or lower the keepalive interval.

- CSCsg29498

  Symptoms: A router may reload when you enter the **show monitor event-trace adjacency all** command.

  Conditions: This symptom is observed when you enter the command after a route to a destination changes from multiple paths to a single path.

  Workaround: There is no workaround.

- CSCsg37435

  Symptoms: The output of the **show snmp mib ifmib ifindex** command does not show the SNMP Interface Index identification numbers (ifIndex values) for 802.1Q VLAN subinterfaces.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router after you have performed an OIR of a Gigabit Ethernet module.

  Workaround: Reload the platform.

- CSCsg44555

  Symptoms: An MPLS TE tunnel with a third-party vendor headend, a Cisco midpoint, and a Cisco tailend may occasionally transition to the up/down state on the midpoint while still appearing in the up/up state on the headend and tailend. When this situation occurs, traffic may continue to flow on the tunnel even though the tunnel is in the up/down state at the midpoint or it may come to a halt.

  Conditions: This symptom is observed when the Cisco router that is the tailend for the MPLS TE tunnel uses a bandwidth or burst size that is not a multiple of 1 Kbps or 1 Kbyte and that rounds up the Resv burst size to the next higher multiple of 1 Kbps or 1 Kbyte.

  Workaround: Specify a tunnel bandwidth that is a multiple of 8 Kbps.

- CSCsg58587

  Symptoms: The “ifHCOutUcastPkts” SNMP output counters for VLANs are incorrect because they count the data twice:

  ```
  interfaces.ifTable.ifEntry.ifOutUcastPkts.xxx : Counter: <=== counted twice
  ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifHCOutUcastPkts.xxx : Counter64: <=== counted twice
  ```

  Conditions: This symptom is observed on a Cisco 7600 series.

  Workaround: There is no workaround.

  Further Problem Description: Note that the “ifHCInUcastPkts” SNMP input counters function fine and provide correct data.

- CSCsg68740

  Symptoms: Fast Reroute (FRR) is not triggered when a cable is removed from a POS SPA or POS OSM, causing data loss of 3 to 4 seconds.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router.

  Workaround: There is no workaround.

  Further Problem Description: This symptom does not occur when a POS port adapter is installed in an Enhanced FlexWAN module.

- CSCsg68783

  Symptoms: The ATM SAR may hang on an ATM interface that is configured for AToM.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when you enter the **clear mpls traffic-eng auto-tunnel mesh** command.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected ATM interface.

  Further Problem Description: The symptom occurs because the ATM SAR receives a packet that is larger than the ATM cell size in the AToM mode of operation.

- CSCsg98612

  Symptoms: The **speed nonegotiate** command does not function for Gigabit Ethernet ports on a SIP-600.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA2 or Release 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCsh42857

  Symptoms: After TE tunnel reoptimization, the AToM traffic is not passing anymore due to a stale outgoing label and interface in the hardware.

  Conditions: This symptom has been observed with AToM circuits going over a TE tunnel.

  Workaround: Enter the **shutdown** command and the **no shutdown** command on the CE facing interface or configure and deconfigure the **xconnect** command on the CE facing interface will reestablish the traffic forwarding until a new reoptimization occurs.

TCP/IP Host-Mode Services

- CSCse05736

  Symptoms: A router that is running RCP can be reloaded by a specific packet.

  Conditions: This symptom is seen under the following conditions:

  - The router must have RCP enabled.
  - The packet must come from the source address of the designated system configured to send RCP packets to the router.
  - The packet must have a specific data content.

  Workaround: Put access lists on the edge of your network blocking RCP packets to prevent spoofed RSH packets. Use another protocol such as SCP. Use VTY ACLs.

- CSCsf33034

  Symptoms: The following error message and tracebacks are generated during the boot process:

```
%TCP-2-INVALIDTCB: Invalid TCB pointer: 0x4704D088
 -Process= "IP Input", ipl= 0, pid= 122
 -Traceback= 409F00FC 409E4C50 407A032C 407D8EAC 4077FF38 407911D0 4078EC2C 4078EDE8
4078F004
```

  Conditions: This symptom is observed on a Cisco platform when a TCP server is configured.

  Workaround: There is no workaround.

  Further Problem Description: A TCP control block that is already freed is referenced or accessed, causing the error message to be generated. This situation does not affect the proper functioning of the platform in any way.

Wide-Area Networking

- CSCek45604

  Symptoms: An OSM or FlexWAN module may crash when you apply an input QoS configuration to a Frame Relay interface in a particular sequence.

  Conditions: This symptom is observed on a Cisco 7600 series when the following sequence of events occurs:

  1. You attach a policy to the main interface and you use the map class for inheritance.
  2. You remove the Frame Relay class from the interface and attach a flat policy to the main interface.

  Note that the symptom does not occur when you apply an output QoS configuration to a Frame Relay interface.

  Workaround: Do not apply an input QoS configuration to a Frame Relay interface.

- CSCsg35429

  Symptoms: Spurious access messages may be generated when you enter the **mpls bgp forwarding** command on a multilink interface.

  Conditions: This symptom is observed on a Cisco router that is configured for PPP.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRA2

Cisco IOS Release 12.2(33)SRA2 is a rebuild release for Cisco IOS Release 12.2(33)SRA. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRA2 but may be open in previous Cisco IOS releases.

IBM Connectivity

- CSCsf28840

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml.

IP Routing Protocols

- CSCsa87034

  Symptoms: When you attempt to clear the routing table, the neighbor is brought down instead.

  Conditions: This symptom is observed when you enter the **clear bgp ipv4 unicast *** or **clear bgp ipv6 unicast *** command, causing respectively the IPv4 neighbor or IPv6 neighbor to be brought down.

  Workaround: There is no workaround.

- CSCsb86987

  Symptoms: A Cisco router may generate tracebacks or may crash when multicast performs an RPF lookup into the BGP table.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and multicast.

  Workaround: There is no workaround.

- CSCse04220

  Symptoms: The BGP table version remains stuck at 1, and the router may crash.

  Conditions: This symptom is observed when you enter the **clear bgp ipv4 uni *** command for IPv4 or the **clear bgp ipv6 uni *** command for IPv6. The symptom may also occur when you enter the **clear bgp nsap uni *** command for a network service access point (NSAP) address family.

  Workaround: Enter the **clear ip bgp *** command to clear the sessions, purge the BGP table, and prevent the router from crashing.

Miscellaneous

- CSCek37222

  Symptoms: Packets are not classified when a service policy is configured with random-detect in the class default.

  Conditions: This symptom is observed on a Cisco 7600 series when the service policy is attached to a Frame Relay interface on an OSM-CT3 line card or OSM-8OC3-POS module. Note that the symptom does not occur when the service policy is attached to a Frame Relay PVC.

Workaround: There is no workaround.

- CSCek47059

  Symptoms: IPv6 packets may be accounted as MPLS packets in the output of the **show interface accounting** command.

  Conditions: This symptom is observed on a Cisco 7600 series when IPv6 addresses are configured on interfaces of an Optical Services Module (OSM) and when IPv6 traffic or a ping is processed.

  Workaround: There is no workaround.

- CSCek47506

  Symptoms: NetFlow Data Export (NDE) stops functioning unexpectedly, a memory allocation failure (MALLOCFAIL) occurs, hardware-switching becomes disabled, and, finally, the Distributed Forwarding Card (DFC) is reset.

  When an SSO switchover occurs and when the DFC has a high NetFlow TCAM utilization, the DFC stops functioning immediately and is eventually reset.

  Conditions: These symptoms are observed on a Cisco 7600 series when NDE is enabled, especially NDE version 8 or NDE version 9.

  Workaround: There is no workaround.

  Further Problem Description: When NDE stops functioning, the export packets continue to be generated and are queued, waiting to be sent. These packets use up the memory and cause the DFC to run out of memory because the memory pool becomes too fragmented.

- CSCek50720

  Symptoms: A router does not report the cause of an error when an ATM SPA does not boot because of a delay-locked loops (DLL) centering failure during SAR initialization.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(18)SXF and that has an ATM SPA that is installed in a SIP-400. The symptom may also affect other releases.

  Workaround: There is no workaround.

- CSCek52892

  Symptoms: An enhanced FlexWAN module or other line card may crash.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for MPLS and OAM.

  Workaround: There is no workaround.

- CSCek54572

  Symptoms: A switch or router may crash when you configure and unconfigure 500 IPSec VTI tunnels two or three times. The symptom does not occur when you configure and unconfigure the tunnels only once.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series.

  Workaround: After you have configured the tunnels, wait for the tunnels to come up before you unconfigure the tunnels.

- CSCsb40304

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCsd43211

  Symptoms: A SIP-200 may crash when it has a channelized SPA that has a multilink bundle, an LFI configuration, and more than two links in the bundle.

  Conditions: This symptom is observed on a Cisco 7600 series when an SSO or RPR+ switchover occurs while traffic is processed near the line rate, that is, at about 75 percent of the line rate.

  Workaround: There is no workaround.

- CSCsd75273

  The Cisco Catalyst 6000 series, 6500 series, and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM installed are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml.

- CSCsd92405

  Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

Cisco IOS is affected by the following vulnerabilities:

- Processing ClientHello messages, documented as Cisco bug ID CSCsb12598
- Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304
- Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link: http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

- CSCse03277

  Symptoms: When a tunnel is removed and reconfigured, the tunnel interface may not come up.

  Conditions: This symptom is observed on a Cisco router that has a tunnel that is configured on a Virtual Tunnel Interface (VTI).

  Workaround: Shut down the tunnel before you unconfigure the IP address of the tunnel interface, disable the VTI tunnel mode, or remove the VTI tunnel itself.

- CSCse12195

  Symptoms: Connected ports on a Cisco Catalyst 6000 series or Cisco 7600 series may transition from the up state to the down state with no apparent cause.

  Conditions: This symptom is observed on a 16-port Gigabit Ethernet GBIC line card (WS-X6816-GBIC) when the following two conditions are met:

  - A 1000Base-T GBIC is inserted after the WS-X6816-GBIC has been powered up.
  - Port 1 is enabled, not connected, and set to auto-negotiate.

  Workaround: Disable auto-negotiation on port 1 by entering the **speed nonegotiate** command.

  First Alternate Workaround: Remove all 1000Base-T GBICs that are in use, reset the WS-X6816-GBIC, and refrain from using 1000Base-T GBICs.

  Second Alternate Workaround: Disable port 1.

- CSCse22153

  Symptoms: The following error messages may be generated on the console of the standby RP when MPLS TE tunnels are deleted and then added while the standby RP reloads.

  ```
  %IDBINDEX_SYNC-STDBY-3-IDBINDEX_ENTRY_LOOKUP: Cannot find IDB index table
  entry: "", 0
  ```

  ```
  %COMMON_FIB-STDBY-2-IF_NUMBER_ILLEGAL: Attempt to create CEF interface for Tunnel5
  with illegal if_number: -1
  ```

  Conditions: This symptom is observed in an MPLS network that has multiple TE tunnels.

  Workaround: Do not delete and add MPLS TE tunnels while the standby RP reloads.

- CSCse41480

  Symptoms: The CoS VLAN priority may be changed and become corrupted when MPLS packets are sent over an EoMPLS tunnel on Cisco 7600 series even when the **mls qos trust cos** command is enabled on the ingress interface.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(18)SXE2 or Release 12.2(18)SXF4 but may also affect other releases that run on the Cisco 7600 series. The symptom occurs only when packets with Ethertype 8847 and 8848 are processed on the ingress interface, causing an incorrect MPLS EXP bit to be assigned on the ingress interface.

  Note that the symptom does not occur when the payload is IP (Ethertype 0800) or any other Ethertype.

  Workaround: There is no workaround. (However, see the Further Problem Description.)

  Further Problem Description: The fix for this caveat does not resolve the underlying hardware issue but, as a workaround, it does allow you to configure an ingress marking policy on the EoMPLS interface, to match on the incoming MPLS EXP bit values (that is, value 0 through 7), and to set the marking to the same value.

- CSCse52951

  The Cisco Catalyst 6000 series, 6500 series, and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM installed are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml.

- CSCse59865

  Symptoms: The “ifDescr” for dot1q encapsulation on the interface of a 1-port 10 Gigabit Ethernet SPA may be truncated and may cause the “ifDescr” to be incorrect or the router to crash.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SRA.

  Workaround: There is no workaround.

- CSCse62462

  Symptoms: When a GRE tunnel is routed over an MPLS cloud, process-switched packets that are destined for the remote end of the GRE tunnel are sent unlabeled.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2S or a release that is based on Release 12.2S when the router functions as a PE router that has a GRE tunnel configured within a VRF that is sourced from another VRF.

  Workaround: There is no workaround.

- CSCse67650

  Symptoms: Non-IP packets may be dropped from an egress interface when a QoS service policy with WRED is applied. Dropped packets may include ARP and MPLS LDP packets. If the router is booted with this configuration, the router may be unable to perform L2 address resolution for IP and fail to establish MPLS neighbor relationships.

  Conditions: This symptom is observed on a Cisco 7600 series when a QoS service policy with WRED is applied to an interface on a SIP-600.

  Workaround: Remove WRED from any QoS policies that are applied on SIP-600 interfaces.

- CSCse74713

  Symptoms: Pings may fail across a link on an ATM SPA that is configured for MLP, LFI, and VRF forwarding and that is installed in a SIP-400.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA.

  Workaround: Reload the router and reapply the VRF configuration to the virtual template.

  Further Problem Description: The symptom does not occur in Release 12.2.18SXF4 and earlier releases.

- CSCse75429

  Symptoms: An LDP neighbor does not come up when the MPLS LDP Graceful Restart feature is enabled.

  Conditions: This symptom is observed when the forwarding state holding timer of the MPLS LDP Graceful Restart feature is configured to a value that is less than 120 seconds, causing the LDP session to be brought down.

  Workaround: Configure the forwarding state holding timer to a value that is greater than or equal to 120 seconds.

- CSCse77427

  Symptoms: The throughput performance may be adversely affected on a Cisco 7600 series that has a SIP-600 in which a 1-port 10 Gigabit Ethernet SPA or 10-port Gigabit Ethernet SPA is installed that is configured for Hierarchical Virtual Private LAN Service (H-VPLS) with traffic engineering (TE) tunnels.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA when the 1-port 10 Gigabit Ethernet SPA or 10-port Gigabit Ethernet SPA processes incoming packets at 50 percent of the line rate and has the TE tunnels disabled after they were previously enabled for the incoming traffic.

  Workaround: There is no workaround.

- CSCse77768

  Symptoms: MAC addresses may not be learned when traffic is switched from Multipoint Bridging (MPB) to Virtual Private LAN Services (VPLS).

  Conditions: This symptom is observed on a Cisco 7600 series when traffic is switched from a customer-facing interface that is configured for MPB on a SIP-400 to a core-facing interface that is configured for VPLS and EoMPLS on a SIP-200, SIP-600, enhanced 4-port Gigabit Ethernet OSM, or FlexWAN2.

  Workaround: There is no workaround.

- CSCse91675

  Symptoms: The RP may generate a RX FIFO FULL error message for a SPA, followed by a VC_CONFIG error message, and subsequently all interfaces on all SPAs that are processing traffic may go down.

  Symptoms: This symptom is observed on a Cisco 7600 series that is configured with MLP or MFR bundles on a 1-port channelized STM1/OC3 to DS0 SPA (SPA-1XCHSTM1/OC3), 2-port channelized T3/DS0 SPA (SPA-2XCT3/DS0), or 4-port channelized T3/DS0 SPA (SPA-4XCT3/DS0) when traffic exceeds about 350 kpps on these bundles.

Workaround: After the symptom has occurred, reload the affected SPAs or the SIPs in which the affected SPAs are installed. There is no workaround to prevent the symptom from occurring. Therefore, configure the MLP or MFR bundles in such a manner that the 350 kpps threshold is not exceeded.

- CSCse94388

  Symptoms: A SIP-200 that is configured with distributed Multilink Point-to-Point (dMLP) bundles and that has some of the bundles interleaved may crash.

  Conditions: This symptom is observed when you send traffic at line rate through all of the bundles.

  Workaround: There is no workaround.

- CSCse95146

  Symptoms: A Supervisor Engine 720 with a cross-module EtherChannel duplicates all packets that enter or leave the cross-module EtherChannel on the same physical port.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series or Cisco 7600 series that has a Supervisor Engine 720 and an Enhanced FlexWAN module when the supervisor engine functions in bus mode and has a cross-module EtherChannel.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur when you remove the cross-module EtherChannel or the Enhanced FlexWAN module.

- CSCse95888

  Symptoms: The bandwidth of an interface on a Fast Ethernet (FE) SPA changes unexpectedly when the interface on the other side is shut down and brought back up, or the other around, brought up and then shut down.

  Conditions: This symptom is observed on a Cisco router such as a Cisco 7600 series or Cisco 12000 series that is configured with an FE SPA.

  Workaround: Use the **bandwidth** command to configure the appropriate bandwidth.

- CSCse98354

  Symptoms: The interfaces of the SPAs on a SIP-200 may enter the up/down state.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(18)SXF5 but may also occur in Release 12.2(33)SR.

  Workaround: There is no workaround.

- CSCsf04301

  Symptoms: All multicast data packets on ATM multipoint interfaces may be dropped, regardless of the number of VCs that are configured under a single multipoint interface. When this situation occurs, control plane packets still pass so that routing protocol adjacencies do come up and PIM neighbors are formed.

  Conditions: This symptom is observed on a Cisco 7600 series that has an ATM SPA.

  Workaround: There is no workaround.

  Further Problem Description: The ATM OSM is able to direct multicast packets to a single VC that is configured on a multipoint interface.

- CSCsf05390

  Symptoms: A Cisco 7600 series that has a 1-port channelized STM1/OC3 to DS0 SPA (SPA-1XCHSTM1/OC3) may generate several CPUHOG messages and may crash.

Conditions: This symptom is observed when you create the 258th channel group on the SPA-1XCHSTM1/OC3 and then delete one of the channel groups.

Workaround: There is no workaround.

- CSCsf11098

  Symptoms: When you insert a 2-port Gigabit Ethernet SPA (SPA-2X1GE-V2) in a SIP-400 on a Cisco 7600 series, the following error messages may be generated:

  ```
  %FPD_MGMT-3-MAJOR_VER_MISMATCH: Major image version mismatch detected with GE I/O
  FPGA (FPD ID=1) for SPA-2X1GE-V2 card in subslot 5/2. Image will need to be upgraded
  from version 0.5 to at least a minimum version of 1.10. Current HW version = 0.21.

  %FPD_MGMT-5-UPGRADE_ATTEMPT: Attempting to automatically upgrade the FPD image (s)
  for SPA-2X1GE-V2 card in subslot 5/2. Use 'show upgrade fpd progress' command to view
  the upgrade progress ...

  %FPD_MGMT-3-PKG_FILE_SEARCH_FAILED: FPD image package (c7600-fpd-pkg.122-
  33.SRA.pkg) cannot be found in system's flash card or disk to do FPD upgrade.

  %FPD_MGMT-3-CARD_DISABLED: SPA-2X1GE-V2 card in subslot 5/2 is being disabled because
  of an incompatible FPD image
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA or Release 12.2(3)SRA1 and occurs because the SPA-2X1GE-V2 is not supported in Release 12.2(33)SRA and its rebuilds.

  Workaround: Do not insert a SPA-2X1GE-V2 in a Cisco 7600 series that runs Release 12.2(33)SRA or one of its rebuilds.

- CSCsf14018

  Symptoms: A router may crash when a large number of VRFs such as 150 or more are unconfigured.

  Conditions: This symptom is observed when the deletion process suspends while deleting a VRF and when another process that is triggered by the timer deletes the same VRF. When the suspended process resumes, the process attempts to free the already freed memory that belonged to the already deleted VRF. This situation causes the router to crash.

  Workaround: There is no workaround.

- CSCsf19575

  Symptoms: A Cisco 7600 series that has an IPsec SPA with mGRE tunnels that function in VRF mode may crash.

  Conditions: This symptom is observed when you enter the **crypto engine slot** *slot/subslot* **inside** command on the mGRE interface.

  Workaround: There is no workaround.

- CSCsf20194

  Symptoms: When you perform an OIR of a SIP-200, the SIP-200 may crash.

  Conditions: This symptom is observed when the same policy map is attached to both the ingress and egress side of an interface on the SIP-200.

  Workaround: There is no workaround.

- CSCsf25712

  Symptoms: A line card such as a SIP-200 may crash when the line card on the other side or SPAs in the line card on the other side are reloaded.

  Conditions: This symptom is observed on a router that has a highly scaled configuration (for example, a configuration that is used for mobile users) with priority traffic and non-priority traffic running at line rate.

Workaround: There is no workaround.

Further Problem Description: The symptom occurs because of memory corruption.

- CSCsf27085

  Symptoms: A SIP-200 may crash when a class with a priority is removed from a service policy while traffic is being processed.

  Conditions: This symptom is observed when the class that is being removed is the last class at a layer in the service policy.

  Workaround: There is no workaround.

- CSCsg04681

  Symptoms: Traffic from an MPLS cloud to a tunnel interface within a VRF may stop when the tunnel interface is moved from the supervisor engine to a SPA.

  Conditions: This symptom is observed on a Cisco 7600 series.

  Workaround: First shut down the tunnel interface, then move the tunnel interface to the SPA, and then bring up the tunnel interface.

- CSCsg17500

  Symptoms: OSPFv3 neighbors or adjacencies are not formed across MLP and MFR links.

  Conditions: This symptom is observed on a Cisco 7600 series for MLP and MFR configurations on a FlexWAN module that is configured for OSPFv3.

  Workaround: There is no workaround.

- CSCsg24278

  Symptoms: After a Supervisor Engine 32 has been powered-on or reloaded, it may enter a state in which it responds very slowly. For example, the response time to a ping from a directly-connected host is very high such as in the order of hundreds of milliseconds as opposed to under a few milliseconds in a normal state.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA1.

  Workaround: There is no workaround.

- CSCsg32195

  Symptoms: Line cards that are equipped with a Distributed Forwarding Card 3A (DFC3A) should be powered down because they are not supported in Cisco IOS Release 12.2(33)SRA, but they are still powered up.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA.

  Workaround: There is no workaround.

- CSCsg35439

  Symptoms: After a switch or router boots up, OSPF neighbors continue to flap. This situation occurs because, even though the switch or router correctly sends and receives OSPF hello packets at every interval, it incorrectly detects that the neighbors are down.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series that has a Supervisor Engine 32 and that runs Cisco IOS Release 12.2(18)SXF6 and on a Cisco 7600 series that has a Supervisor Engine 32 and that runs Release 12.2(18)SXF6 or Release 12.2(33)SRA1.

  Workaround: There is no workaround.

- CSCsg38930

  Symptoms: IP fragments may not be forwarded over an GRE tunnel when the tunnel is configured to go through an IPSEC-SPA-2G. These IP fragments may be dropped.

  Conditions: This symptom is observed on a Cisco 7600 series that has a Supervisor Engine 720 and an IPSEC-SPA-2G, and that runs Cisco IOS Release 12.2(18)SXF5 when the tunnel is configured in the following manner:

  – Path MTU Discovery (PMTUD) is enabled.
  – IPsec tunnel protection is enabled.
  – The **crypto engine slot** *slot/subslot* **inside** command is enabled.

  The symptom may also affect other releases.

  The output of the **show crypto vlan** command shows the VLAN that is associated with the crypto configuration.

  Temporary Workaround: Use an ACL with an ACE and the **log** keyword for the specific multicast group.

  Workaround: Disable Path MTU Discovery (PMTUD).

- CSCsg46087

  Symptoms: A packet with a size that is larger than 1460 bytes does not go through a GRE IPsec tunnel even when the IP MTU for the tunnel has a size that is larger than the size of the packet (for example, when the IP MTU is set to 1514 bytes).

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series and Cisco 7600 series that are configured with an IPSEC-SPA-2G SPA when the following conditions are present:

  – Path MTU Discovery (PMTUD) is enabled.
  – The DF bit is set for the tunnel interface.

  Workaround: Disable PMTUD.

  First Alternate Workaround: Do not set the DF bit for the tunnel interface.

  Second Alternate Workaround: Use a small IP MTU for the tunnel.

  Further Problem Description: Enabling fragmentation on a large number of tunnels may cause some packet loss due to fragmentation timeouts.

- CSCsg46761

  Symptoms: A Cisco 7600 series may reload, causing a temporary service outage.

  Conditions: This symptom is observed when the following conditions are present:

  – The router contains a SIP-600.
  – The SIP-600 contains a Shared Port Adapter (SPA).
  – One or more of the plugholes in the SPA do not contain Small Form Factor Pluggable (SFP) modules.
  – You enter the **show interface transceiver** command at the router console.

  Workaround: Do not enter the **show interface transceiver** command unless all plugholes in all SPAs in the SIP-600 contain SFP modules.

- CSCsg85046

  Symptoms: A Cisco 7600 series with a SIP-600 crashes during the boot process.

Conditions: This symptom is observed only when a 4-port OC-48c/STM-16 POS/DPT/RPR SPA (SPA-4XOC48POS/RPR) is installed in the SIP-600.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRA1

Cisco IOS Release 12.2(33)SRA1 is a rebuild release for Cisco IOS Release 12.2(33)SRA. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRA1 but may be open in previous Cisco IOS releases.

IP Routing Protocols

- CSCek38025

  Symptoms: A Multicast Distribution Tree (MDT) update does not reach a remote PE router.

  Conditions: This symptom is observed when some of the routers in the network core send MDT addresses in the form of VPNv4 extended community attributes and other routers in the network core send MDT addresses in the MDT SAFI format.

  Workaround: Configure all routers in the network core to use only one form of MDT implementation (that is, configure either the VPNv4 extended community format or the MDT SAFI format).

- CSCek45564

  Symptoms: A router crashes because of memory corruption when you bring up Gigabit Ethernet links and BGP neighbor adjacencies, and an error message is generated, indicating that a block overrun and rezone corruption have occurred.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7600 series that are configured for BGP.

  Workaround: There is no workaround.

- CSCsd98168

  Symptoms: A router may reload unexpectedly when you enable the BGP Support for TCP Path MTU Discovery per Session feature in session-template configuration mode.

  Conditions: This symptom is observed on a Cisco router when there are no BGP neighbors configured.

  Workaround: On a router has no BGP neighbors, do not enable the BGP Support for TCP Path MTU Discovery per Session feature in session-template configuration mode, nor enter the **no transport path-mtu-discovery** command session-template configuration mode.

Miscellaneous

- CSCek31437

  Symptoms: A WS-6516-GE-TX module may not power up, and the following error message may be generated:

  ```
  C6KPWR-SP-4-UNSUPPORTED: unsupported module in slot <slot-no>, power not allowed:
  Module not at an appropriate hardware revision level.
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that are configured with a Supervisor Engine 32 that runs Cisco IOS Release 12.2SR or Release 12.2SX.

Workaround: There is no workaround.

- CSCek35061

  Symptoms: A router may crash when you disassociate a VRF from an MPLS interface.

  Conditions: This symptom is observed on a Cisco router that is configured for L2TP when you enter the **no ip vrf forwarding** *vrf-name* command.

  Workaround: There is no workaround.

- CSCek45862

  Symptoms: Packets are not classified according to the value of the *mpls-exp-value* argument in the **set mpls experimental imposition** *mpls-exp-value* command.

  Conditions: This symptom is observed on a Cisco 7600 series that functions as a 6PE router when packets are processed via a SIP-200.

  Workaround: There is no workaround.

- CSCek47083

  Symptoms: In a blade-to-blade configuration, when the encryption cards are reloaded at the same time, there are less GRE SAs at the active blade than that there are at the standby blade, causing traffic loss for the GREs that are missing from the active blade.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in a blade-to-blade redundancy configuration and that has 500 GRE over IPsec tunnels.

  Workaround: Do not reload both encryption cards at the same time. First reload one encryption card and wait until it has come up. Then, reload the other encryption card.

- CSCek47205

  Symptoms: A Cisco 7600 series may crash when a blade-to-blade switchover occurs.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.3(33)SRA, that has an IPSec VPN SPA, and that has the **crypto engine mode vrf** command enabled.

  Workaround: There is no workaround.

- CSCek48618

  Symptoms: A Cisco 7600 series may generate the following error message in the console log:

```
%FPD_MGMT-4-UPGRADE_EXIT: Unexpected exit of FPD image upgrade operation for
7600-SSC-400 card in slot 4.
```

  After this error message, the following error messages are generated, indicating that the 7600-SSC-400 is unable to boot:

```
%C6KPWR-SP-4-DISABLED: power to module in slot 4 set off (Reset - Module Reloaded
During Download)
%OIR-SP-3-PWRCYCLE: Card in module 4, is being power-cycled off (Reset - Module
Reloaded During Download)
%C6KPWR-SP-4-DISABLED: power to module in slot 4 set off (Reset - Module Reloaded
During Download)
%OIR-SP-3-PWRCYCLE: Card in module 4, is being power-cycled off (Reset - Module
Reloaded During Download)
%C6KPWR-SP-4-DISABLED: power to module in slot 4 set off (Reset - Module Reloaded
During Download)
%OIR-SP-3-PWRCYCLE: Card in module 4, is being power-cycled off (Reset - Module
Reloaded During Download)
```

```
%C6KPWR-SP-4-DISABLED: power to module in slot 4 set off (Reset - Module Reloaded
During Download)
%OIR-SP-3-PWRCYCLE: Card in module 4, is being power-cycled off (Reset - Module
Reloaded During Download)
%C6KPWR-SP-4-DISABLED: power to module in slot 4 set off (Reset - Module Reloaded
During Download)
%CWAN_RP-3-BOOTFAIL: The WAN module in slot 4/0 failed to boot
%OIR-SP-3-PWRCYCLE: Card in module 4, is being power-cycled off (Reset - Module
Reloaded During Download)
%CWAN_RP-3-BOOTFAIL: The WAN module in slot 4/0 failed to boot
%CWAN_RP-3-RESET_FAIL: The WAN module in slot 4 failed even after several resets
```

Workaround: Contact Cisco TAC for a workaround that prevents an RMA of the 7600-SSC-400.

- CSCsc38127

  Symptoms: The standby supervisor engine may crash when an interface has a stateful inspection policy or when the **ip nbar protocol-discovery** command is enabled.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series or Cisco 7600 series that run a native Cisco IOS software image.

  Workaround: There is no workaround.

- CSCsd39344

  Symptoms: When MPLS cell-relay or ATM cell-switched traffic enters an OC-48 ATM SPA that is installed in a SIP-400, the performance is limited to 64.5 percent of the OC-48 line rate (which is about 1.5 Gb/s).

  Conditions: This symptom is observed on a Cisco 7600 series and occurs only for MPLS cell-relay or ATM cell-switched traffic.

  Workaround: Avoid sending MPLS cell-relay or ATM cell-switched traffic above 64.5 percent of the OC-48 line rate to the OC-48 ATM SPA.

  Note that the performance for two-cell traffic or traffic with larger packets (that is, non-cell switched traffic) is not impacted and full line rate is supported in these cases.

- CSCsd96511

  Symptoms: When a hardware interface goes down, for example because the interface is shut down, the cable is disconnected, or an uplink on a supervisor engine goes from the active state to the standby state, packets in the egress direction are bridged in the software for later processing. When there is a high traffic rate, this situation may cause CPU congestion until the routing table is updated in the hardware. This type of traffic (that is, traffic that is bridged for later processing) cannot be rate-limited.

  Conditions: This symptom is observed on a Cisco 7600 series.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat causes the packets to be denied and dropped instead of being bridged in the software.

- CSCse00135

  Symptoms: When MLPoMPLS is configured, a VC comes up but, the first few ping packets from one CE router to another CE router on the far end do not go through.

  Conditions: This symptom is observed in a configuration with Cisco 7600 series routers that functions as CE and PE routers.

  Workaround: There is no workaround. Note that the connectivity recovers after a few pings.

- CSCse05336

  Symptoms: A subinterface of an OSM-2+4GE-WAN+ that is passing traffic may drop some packets when you create a new subinterface or delete an existing subinterface on the same physical interface as the subinterface that is passing traffic.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that are configured with a Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXF3. The symptom may also affect Release 12.2(33)SRA.

  Workaround: There is no workaround.

- CSCse14269

  Symptoms: The encapsulation and decapsulation counters in the output of the **show crypto ipsec sa stats** command are inaccurate because they are not updated correctly during a rekey.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with an IPsec VPN SPA.

  Workaround: Do no set the IPsec SA lifetime to prevent rekeying of the IPsec SA.

- CSCse19351

  Symptoms: On a Cisco 7600 series that has an IPsec VPN SPA, traffic may not pass through an IPsec tunnel when the destination is reached through a front-door VRF (FVRF).

  The symptom typically occurs in the following configuration:

```
interface Tunnel105
 ip vrf forwarding black
 ip address 10.0.0.1 255.0.0.0
 tunnel source 10.0.1.1
 tunnel destination 10.0.0.2
 tunnel vrf temp2044
 tunnel protection ipsec profile ipsec_black_105
 crypto engine slot 3/0 inside
```

  Conditions: This symptom is observed when the internal VRF table ID that is associated with a FVRF is greater than 1024.

  In the example above (in the Symptoms section), the internal VRF table ID that must be confirmed is “temp2044”; enter the **show ip vrf detail temp2044** command to identify the internal VRF table ID.

  Workaround: Limit the number of VRFs that are defined on the router to less than 1024.

- CSCse20150

  Symptoms: A SPA may cause an RX FIFO FULL error message to be generated on the RP. When this occurs, a VC_CONFIG error message is generated, and subsequently all interfaces on all SPAs that are switching traffic go down.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for MLP or MFR when traffic with 46-byte size packets exceeds about 350 kpps on the MLP or MFR bundles.

  Workaround: When the symptom has occurred, reload the SIP with the affected SPA. To prevent the symptom from occurring, ensure that traffic does not exceed about 350 kpps on the MLP or MFR bundles. If this is not an option, there is no preventive workaround.

  Further Problem Description: The following is an example configuration in which the symptom occurs:

Consider 110 bundles with 6 members with 4 DS0 interfaces, so each bundle has 1.5 Mbps of bandwidth. When you send an IP packet of 46 bytes, the maximum traffic that will flow through the SIP is as follows:

```
110 Bundles * (1536kbps * 1000bits) / (8 * (46bytes + 13bytes)) = 357965 pps (rounded
to about 350 kpps)
```

- CSCse20340

  Symptoms: Upon recovery from a microcode reload on a line card or a router bootup, the controller state for a serial interface of a 2-port or 4-port T3/E3 SPA may remain in the “down” state.

  Conditions: This symptom is observed on a Cisco 7600 series and Cisco 12000 series.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected serial interface to enable the interface to enter the “up” state.

- CSCse30293

  Symptoms: A ping may not go through an IPsec tunnel on a Cisco 7600 series after you have copied a configuration from a disk device to the running configuration.

  Conditions: This symptom is observed on a Cisco 7600 series system that has an IPsec VPN SPA on which tunnels with tunnel protection are configured.

  When the symptom occurs, the encryption and decryption counters in the output of the **show crypto ipsec sa** command for the affected IPsec tunnel do still increment, but a ping to the tunnel IP address does not go through. The output of the **show interface tunnel** *number* shows the tunnel interface.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected tunnel interface.

- CSCse34615

  Symptoms: A RADIUS virtual server drops RADIUS accounting on and off packets, instead of forwarding the packets to the real servers. The client never receives response packets for the RADIUS accounting on and off packets that were sent.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7600 series.

  Workaround: There is no workaround.

- CSCse35278

  Symptoms: A Cisco 7600 series with an IPSec VPN Services Module or IPSec VPN SPA may incorrectly drop IPSec NAT Traversal (NAT-T) transit packets that are transported via UDP port 4500.

  Conditions: This symptom is observed on a Cisco 7600 series that terminates IPSec tunnels on an IPSec VPN Services Module or IPSec VPN SPA when the NAT-T packets must traverse the crypto VLAN.

  Workaround: There is no workaround.

- CSCse35319

  Symptoms: The IP MTU is not properly applied to the payload.

  Conditions: This symptom is observed when the IP MTU is configured on a Virtual Tunnel Interface (VTI).

  Workaround: There is no workaround.

- CSCse35622

  Symptoms: Routed packets are dropped from VLANs that are configured for split horizon.

Conditions: This symptom is observed on a Cisco 7600 series that is configured with a SIP-400 when two or more VLANS are configured for split horizon and when a layer-3 packet is routed from one VLAN with a split horizon configuration to another VLAN with a split horizon configuration.

Workaround: Do not configure split horizon, which is a bridge-domain option, on an interface or subinterface when layer-3 traffic may be routed from another bridge domain that is configured with split horizon. Note that this workaround disables the split horizon feature for bridging, which is its normal use.

Further Problem Description: The symptom occurs on a SIP-400 because the line card microcode does not distinguish between layer-2 switched packets and layer-3 routed packets on bridged interfaces when split horizon is configured. Both cases result in dropped packets, which is correct for layer-2 switched packets but not for layer-3 routed packets.

- CSCse47732

  Symptoms: RFC 1407 and RFC 2496 are not supported on a 1-port channelized STM1/OC3 SPA.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA when SNMP queries are performed for CISCO-DS3-MIB objects.

  Workaround: There is no workaround.

- CSCse50009

  Symptoms: The supervisor engine of a Cisco 7600 series may generate the following error message:

  ```
  %COMMON_FIB-SP-3-FIBXDRINV: Invalid XDR format. FIB entry XDR has bogus routecount
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for IPv6 when you configure a PortChannel.

  Workaround: There is no workaround.

- CSCse50607

  Symptoms: Periods of high latency may occur on a Multilink PPP interface, and finally the interface may lock up.

  Conditions: This symptom is observed on a Cisco 7600 series when the Multilink PPP interface is configured on a SPA-8XCHT1/E1 that is installed in a SIP-200.

  Workaround: Configure multilink interfaces on another line card that does not require insertion in a SIP.

  Alternate Workaround: Configure IP load balancing by using two separate E1 links (that is, do not use multilink interfaces).

- CSCse57865

  Symptoms: An ICMP unreachable message from an IPsec VPN SPA does not have the correct MTU size. The MTU value is too conservative and causes an unexpected fragmentation behavior for traffic within a specific packet-size range.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA when traffic is sent that has the DF bit set and that must be fragmented after the IPsec encryption.

  Workaround: There is no workaround.

- CSCse73539

  Symptoms: A Supervisor Engine 720 may crash because the EOBC channel is jammed when you insert a second Supervisor Engine 720 in the chassis.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and a Cisco 7600 series.

Workaround: There is no workaround.

- CSCse76036

  Symptoms: In an MPLS TE FRR configuration, a point of local repair (PLR) router may insert an MPLS label that has a value of 3 (that is, an implicit null label) into the outgoing label stack. This situation prevents traffic from being forwarded.

  Conditions: This symptom is observed on a Cisco 7600 series when the primary TE tunnel is a one-hop tunnel that is configured for implicit null labels and LDP. For an MPLS L3VPN prefix, the outgoing packets have a label stack of "3, ldp label, vpn label." The correct label stack in this case should be "ldp label, vpn label."

  Workaround: Configure the one-hop primary TE tunnel for explicit-null labels as the outgoing labels.

- CSCsf04112

  Symptoms: On a Cisco 7600 router, the MAC address of one or more interfaces may change unexpectedly when the ifPhysAddress object of the IF-MIB is accessed by SNMP. This situation prevents the router from receiving packets when an ARP entry that contains the MAC address of the router is refreshed.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA.

  Workaround: To prevent the symptom from occurring, configure static ARP on the devices that must be able to send packets to the router. After the symptom has occurred, reload the router to clear the condition.

- CSCsf04754

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

  The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

  Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

  This advisory will be posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml

- CSCsf13513

  Symptoms: Packets are dropped because of decryption errors.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that are configured with an SPA-IPSEC-2G and occurs when incoming NAT-T packets result in an error. This situation causes incorrect information to be sent with the next packet, and, in turn, causes a decryption error.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs intermittently, and the platform may recover automatically.

Wide-Area Networking

- CSCek26657

  Symptoms: The following state mismatch error messages may be generated on the console of a standby RP:

  ```
  %IPV6-STDBY-4-IDB: Interface XXX state mismatch. IPv6 state is down, interface is up
  ```

  (Note that XXX represents the interface.)

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with redundant RPs that function in SSO mode, and that is configured for IPv6, PPP, and IP header compression.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(33)SRA

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(33)SRA. All the caveats listed in this section are open in Cisco IOS Release 12.2(33)SRA. This section describes only severity 1, severity 2, and select severity 3 caveats.

IP Routing Protocols

- CSCsb86987

  Symptoms: A Cisco router may generate tracebacks or may crash when multicast performs an RPF lookup into the BGP table.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and multicast.

  Workaround: There is no workaround.

- CSCsc58030

  Symptoms: When a local PE router receives remote VPNv4 routes, the following error messages may be generated.

  ```
  %IPRT-3-PATHIDX: Bad path pointer of 0 for 201.1.10.0, 2 max
  -Process= "BGP Router", ipl= 0, pid= 414
  ```

  Conditions: This symptom is observed on a Cisco router that functions as a PE router with 200 VRFs and about 50,000 VPNv4 routes.

  Workaround: There is no workaround.

- CSCsc79722

  Symptoms: eBGP sessions between a PE router and a CE router may go down after an SSO switchover has occurred.

  Conditions: This symptom is observed after an SSO switchover has occurred on a PE router when the BGP sessions are all set and when all routes in the BGP VPNv4 table have been checked. When you sent traffic from a CE router to the PE router, the BGP sessions may go down after 3 or 4 minutes.

  Workaround: Stop the traffic to enable the eBGP sessions to come up again. Then, resume the traffic.

- CSCsd98168

  Symptoms: A router may reload unexpectedly when you enable the BGP Support for TCP Path MTU Discovery per Session feature in session-template configuration mode.

Conditions: This symptom is observed on a Cisco router when there are no BGP neighbors configured.

Workaround: On a router has no BGP neighbors, do not enable the BGP Support for TCP Path MTU Discovery per Session feature in session-template configuration mode, nor enter the **no transport path-mtu-discovery** command session-template configuration mode.

- CSCse28676

  Symptoms: The following error message may be generated continuously on a PE router, preventing an OSPF neighbor to enter the "Full" state because OSPF packets are dropped:

  ```
  %OSPF-4-BADLENGTH: Invalid length in OSPF packet type x
  ```

  Conditions: This symptom is observed on a Cisco platform that functions as a PE router when the following configuration is present:

  - The OSPF Sham-Link Support for MPLS VPN feature is enabled.
  - The value of the MPLS MTU is smaller than the default MPLS MTU for the connection between the PE router and a P router that functions as the OSPF neighbor.

  Workaround: Configure the default MPLS MTU for the connection between the PE router and the P router.

- CSCse35654

  Symptoms: IPv6 multicast streams may become stuck in the registering state.

  Conditions: This symptom is observed on a Cisco router that has a large number of IPv6 multicast streams.

  Workaround: There is no workaround.

Miscellaneous

- CSCek36924

  Symptoms: Traffic on tunnel interfaces may be punted to the RP.

  Conditions: This symptom is observed on a Cisco 7600 series when you delete and re-create tunnel interfaces. The symptom may not be platform-specific.

  Workaround: There is no workaround.

- CSCek43849

  Symptoms: Traffic on a 4-port Gigabit Ethernet WAN Optical Services Module (OSM-2+4GE-WAN+) may be interrupted.

  Conditions: This symptom is observed on a Cisco 7600 series after you have reloaded the router and when the OSM-2+4GE-WAN+ has an egress HQoS policy. The symptom occurs because the queues on the line card are not created.

  Workaround: Remove and re-apply the policy map on the GE interfaces of the OSM-2+4GE-WAN+.

- CSCek45604

  Symptoms: An OSM or FlexWAN module may crash when you apply an input QoS configuration to a Frame Relay interface in a particular sequence.

Conditions: This symptom is observed on a Cisco 7600 series when the following sequence of events occurs:

1. You attach a policy to the main interface and you use the map class for inheritance.
2. You remove the Frame Relay class from the interface and attach a flat policy to the main interface.

Note that the symptom does not occur when you apply an output QoS configuration to a Frame Relay interface.

Workaround: Do not apply an input QoS configuration to a Frame Relay interface.

- CSCsd39344

  Symptoms: When MPLS cell-relay or ATM cell-switched traffic enters an OC-48 ATM SPA that is installed in a SIP-400, the performance is limited to 64.5 percent of the OC-48 line rate (which is about 1.5 Gb/s).

  Conditions: This symptom is observed on a Cisco 7600 series and occurs only for MPLS cell-relay or ATM cell-switched traffic.

  Workaround: Avoid sending MPLS cell-relay or ATM cell-switched traffic above 64.5 percent of the OC-48 line rate to the OC-48 ATM SPA.

  Note that the performance for two-cell traffic or traffic with larger packets (that is, non-cell switched traffic) is not impacted and full line rate is supported in these cases.

- CSCsd73577

  Symptoms: When the active supervisor engine is reloaded during an SSO switchover, the following error message may be generated:

  ```
  %MDT-4-RD_CONFLICT: MDT entry 10:30:(2.2.2.2,0.0.0.0) received an update for RD 11:30
  ```

  Conditions: This symptom is observed on a Cisco platform that is configured for Multicast VPN.

  Workaround: There is no workaround.

- CSCsd88478

  Symptoms: Memory fragmentation and memory allocation (Malloc) failures may occur on AToM edge or core line cards after a few SSO switchovers have occurred under stress traffic conditions.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR and that has AToM configured when there are several thousand EoMPLS and FRoMPLS or ATMoMPLS VCs configured.

  Workaround: Reload the affected line cards.

- CSCsd99417

  Symptoms: An FRR failover may fail when the primary path for a TE tunnel that is protected by FRR is shut down before the tunnel has completely recovered from a previous FRR failover.

  Conditions: This symptom is observed on a Cisco 7600 series when the primary path fails before the tunnel has reoptimized completely to its primary path. This situation is considered a double failure case and is not supported. The output of the **show mpls traffic-eng fast-reroute database** command shows whether or not the primary tunnel has recovered completely: the FRR database entry should be in the “ready” state for the FRR failover to be successful.

  Workaround: To prevent the symptom from occurring, ensure that the primary path for the TE tunnel that is protected by FRR is not shut down while the tunnel is recovering from a previous FRR failover. When the symptom has occurred, toggle the primary tunnel interface to recover from the failure.

- CSCse19299

  Symptoms: Some packet drops may occur during SA negotiation between two spokes. The expected behavior is that during SA negotiation between the spokes, the traffic should flow through spoke-to-hub tunnels. Note that when the spoke-to-spoke SA is up, traffic flows fine without any packet drops.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR.

  Workaround: There is no workaround.

- CSCse22894

  Symptoms: A traceback and the following error message are generated during the initial boot process:

  ```
  PM-SP-STDBY-3-INTERNALERROR: Port Manager Internal Software Error
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that are configured with two Supervisor Engine 720 processors that run in SSO mode.

  Workaround: There is no workaround.

- CSCse24715

  Symptoms: When Multicast Listener Discovery (MLD) leave messages are sent for 500 or more subinterfaces, traffic continues to be forwarded to some of these subinterfaces.

  Conditions: This symptom is observed on a Cisco 7600 series that sends MLD leave messages via one physical connection to 500 or more subinterfaces. The symptom occurs because some OIFs through which the MLD leave messages are sent are not deleted.

  Workaround: There is no workaround to prevent the symptom from occurring. To recover from the symptom, clear the MFIB entry through which the traffic is forwarded.

  Further Problem Description: This caveat occurs because of a timing issue.

- CSCse31859

  Symptoms: The **monitor session** *session* **destination interface** *type*/*slot*/*port* command does not function.

  Conditions: This symptom is observed on a Cisco 7600 series after you have configured a Remote SPAN (RSPAN) VLAN.

  Workaround: There is no workaround.

- CSCse34025

  Symptoms: When you scale a router with the maximum number (65,536) of dynamic MAC entries, one or two dynamic MAC entries are dropped after a few seconds. You can verify this situation in the output of the **show mac-address-table count** command.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in a basic configuration.

  Workaround: There is no workaround.

- CSCse34697

  Symptoms: When you configure a crypto map and enter the **reverse-route remote-peer** command, the reverse route that is injected by IPsec when the IPsec tunnel comes up may point to an incorrect interface.

Conditions: This symptom is observed when the following occurs:

1. You apply a crypto map to one interface (A).
2. You apply a crypto map to a second interface (B).
3. You remove the crypto map from the second interface (B).

In this situation, when the IPsec tunnel comes up, IPsec points to the second interface (B) instead of the first interface (A).

Workaround: To ensure that the reverse route points to the correct interface, re-apply the crypto map to the first interface (A).

- CSCse35319

  Symptoms: The IP MTU is not properly applied to the payload.

  Conditions: This symptom is observed when the IP MTU is configured on a Virtual Tunnel Interface (VTI).

  Workaround: There is no workaround.

- CSCse35457

  Symptoms: A SPA-8XCTE1 may generate the following error messages during its boot process:

  ```
  %INTR_MGR-3-INTR: SPA-8XCHT1/E1[1/2] [SPA FPGA] IPC RX Parity Error
  %INTR_MGR-3-BURST: SPA-8XCHT1/E1[1/2] [SPA FPGA] IPC TX Parity Error [100]
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that has a SPA-8XCTE1 installed in a SIP-200 and occurs during the boot process of the SPA-8XCTE1.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur after the SPA has properly booted.

- CSCse35825

  Symptoms: An IPsec VPN SPA may become stuck in the “Initializing” state.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that are reloaded with the maximum number of VLANS allocated.

  Workaround: Delete some VLANs or IPsec tunnels to enable the IPsec VPN SPA to enter the “Active” state.

  Further Problem Description: When the symptom occurs, the output of the **show platform hardware capacity | i VLAN** command shows “0 free” VLAN resources:

  ```
  VLANs: 4094 total, 1005 VTP, 0 extended, 3089 internal, 0 free
  ```

  When the platform reloads, the startup configuration allocates all VLANs. While the IPsec VPN SPA boots, there are no VLANs available for the control messaging of the IPsec VPN SPA, causing the IPsec VPN SPA to become stuck in the “Initializing” state.

- CSCse37684

  Symptoms: When an SSO switchover occurs after the STP mode has been changed, some tracebacks may be generated on the newly active supervisor engine.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with two supervisor engines that run in SSO mode.

  Workaround: There is no workaround. However, the tracebacks appear for only about a second and should not affect any functionality of the router.

- CSCse38650

  Symptoms: A router that functions as a BGP Route Reflector in an multicast VPN environment may displays error messages and may eventually crash.

  Conditions: This symptom is observed when the router receives multicast updates and attempts to send multicast updates in which it sets itself as the next hop.

  Workaround: There is no workaround.

- CSCse50009

  Symptoms: The supervisor engine of a Cisco 7600 series may generate the following error message:

  ```
  %COMMON_FIB-SP-3-FIBXDRINV: Invalid XDR format. FIB entry XDR has bogus routecount
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for IPv6 when you configure a PortChannel.

  Workaround: There is no workaround.

- CSCse53249

  Symptoms: A router may crash during the configuration of PIM, specifically when you enter the **ip pim send-rp-announce** command for a tunnel.

  Conditions: This condition is observed on a Cisco router when the following conditions are present:

  – A large number (125 or a higher number) of tunnels is configured.

  – The **ip pim sparse-dense-mode** command is enabled on a VLAN interface.

  – You enter the **ip pim send-rp-announce** *interface-type interface-number* **scope** *ttl-value* command for each tunnel.

  Workaround: Perform the following steps:

  1. Remove the **ip pim sparse-dense-mode** command from the VLAN interface.
  2. Do not enter the **ip pim send-rp-announce** command. Rather, manually configure a rendezvous point (RP) for each scope.

- CSCsg09423

  Symptoms: When IPsec SAs flap, traffic loss may occur during the IPsec and IKE rekey.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA when there is a large number of IKE and IPsec SAs (that is, more than 2000 IKE SAs and 4000 IPsec SAs) and when RSA signature authentication is configured.

  Workaround: Reduce the number of IKE and IPsec SAs.

Resolved Caveats—Cisco IOS Release 12.2(33)SRA

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(33)SRA. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsd75273

  The Cisco Catalyst 6000 series, 6500 series, and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM installed are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml.

- CSCse52951

  The Cisco Catalyst 6000 series, 6500 series, and Cisco 7600 series that have a Network Analysis Module installed are vulnerable to an attack, which could allow an attacker to gain complete control of the system. Only Cisco Catalyst systems that have a NAM installed are affected. This vulnerability affects systems that run Cisco IOS or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml.

Troubleshooting

The following documents provide assistance with troubleshooting your Cisco hardware and software:

- *Hardware Troubleshooting Index Page*:

  http://www.cisco.com/warp/public/108/index.shtml

- *Troubleshooting Bus Error Exceptions*:

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

- *Why Does My Router Lose Its Configuration During Reboot?*:

  http://www.cisco.com/warp/public/63/lose_config_6201.html

- *Troubleshooting Router Hangs*:

  http://www.cisco.com/warp/public/63/why_hang.html

- *Troubleshooting Memory Problems*:

  http://www.cisco.com/warp/public/63/mallocfail.shtml

- *Troubleshooting High CPU Utilization on Cisco Routers*:

  http://www.cisco.com/warp/public/63/highcpu.html

- *Troubleshooting Router Crashes*:

  http://www.cisco.com/warp/public/122/crashes_router_troubleshooting.shtml

- *Using CAR During DOS Attacks*:

  http://www.cisco.com/warp/public/63/car_rate_limit_icmp.html

Related Documentation

The following sections describe the documentation available for Cisco IOS Release 12.2SR. These documents consist of hardware and software installation guides, Cisco IOS configuration and command reference publications, system error messages, feature modules, and other documents.

Documentation is available online on Cisco.com.

Use these release notes with the following resources:

Release-Specific Documents

This section provides information about release-specific documents.

Cisco IOS Release 12.2SR

The following documents are specific to Cisco IOS Release 12.2SR and are located at http://www.cisco.com/univercd/home/index.htm:

- New Feature Documentation for Cisco IOS Release 12.2SR

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/index.htm
- Command Reference for Cisco IOS Release 12.2SR

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/cr/index.htm

Note For Cisco IOS Release 12.2(33)SRA and later releases of Release 12.2SR, all commands that are supported on the Cisco 7600 series are documented in the *Command Reference for Cisco IOS Release 12.2SR*. The *Cisco 7600 Series Router Cisco IOS Command Reference* is still available in Release 12.2(33)SRA but will not be updated for later releases of Release 12.2SR. We recommend that you start using the *Command Reference for Cisco IOS Release 12.2SR*.

Cisco IOS Release 12.2

The following documents are specific to Cisco IOS Release 12.2 and are located on Cisco.com and at http://www.cisco.com/univercd/home/index.htm:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2*

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**: **Release Notes**

  On http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **Release Notes**: **Cisco IOS Release 12.2**

- Configuration guides, command references, system message guides, product bulletins, field notices, and other release-specific documents

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**

  On http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**

- Caveats for Cisco IOS Release 12.2 (Parts 5 through 8)

  As a supplement to the caveats included with these release notes, see the *Cross-Platform Release Notes for Cisco IOS Release 12.2*, which contain caveats applicable to all platforms for all maintenance releases of Release 12.2.

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**: **Release Notes**

  On http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **Release Notes**: **Cisco IOS Release 12.2**

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 **Support: Tools & Resources: Bug Toolkit** (which is listed under Troubleshooting). Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may 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.)

Cisco IOS Release 12.2S

The following documents are specific to Cisco IOS Release 12.2S and are located on Cisco.com and at http://www.cisco.com/univercd/home/index.htm:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2S*

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 S**: **Release Notes**

  On http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **Release Notes**

- New Feature Documentation

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 S**: **Feature Guides**

On http://www.cisco.com/univercd/home/index.htm at

Cisco IOS Software: **Release 12.2**: **New Feature Documentation**: **Cisco IOS Release 12.2 S**: **New Feature Documentation**

- Configuration guides, command references, system message guides, product bulletins, field notices, and other release-specific documents

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 S**

  On http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **New Feature Documentation**: **Cisco IOS Release 12.2 S**: **System Messages for 12.2S**

Cisco IOS Release 12.2SX

The following documents are specific to Cisco IOS Release 12.2SX and are located on Cisco.com and at http://www.cisco.com/univercd/home/index.htm:

- *Release Notes for Cisco IOS Release 12.2SX*

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 SX**: **Release Notes**

  On http://www.cisco.com/univercd/home/index.htm at

  Routers: **Cisco 7600**: **Cisco IOS Software Release Notes**

- New Feature Documentation

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 SX**: **Feature Guides**

  On http://www.cisco.com/univercd/home/index.htm at

  Routers: **Cisco 7600**: **Cisco IOS Software Documentation**: **Cisco 7600 Series Router Cisco IOS Software Documentation, 12.2SX**: **12.2 SX New Features**

- Configuration guides, command references, system message guides, product bulletins, field notices, and other release-specific documents

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 SX**

  On http://www.cisco.com/univercd/home/index.htm at

  Routers: **Cisco 7600**: **Cisco IOS Software Documentation**: **Cisco 7600 Series Router Cisco IOS Software Documentation, 12.2SX**

Platform-Specific Documents

Platform-specific information and documents for the Cisco 7600 series routers are available at the following locations:

- Cisco 7600 series home page on Cisco.com at

  Products & Solutions: **Products: Routers and Routing Systems**: **7600 Series Routers**

- Cisco 7600 series technical documentation on Cisco.com at

  Products & Solutions: **Products: Routers and Routing Systems**: **7600 Series Routers**: in the "Technical Documentation & Tools" box on the right of the page, **Cisco 7600 Series Routers**

- For Cisco 7600 series technical documentation on http://www.cisco.com/univercd/home/index.htm, select **Cisco 7600** from the **Routers** pull-down menu on the top left of the page.

- Cisco 7200 series home page on Cisco.com at

  Support: Select a Product: Routers: Cisco 7200 Series Routers

- Cisco 7200 series technical documenation on Cisco.com at

  Support: Select a Product: Routers: Cisco 7200 Series Routers: Install and Upgrade: Install and Upgrade Guides

- Cisco 7300 series home page on Cisco.com at

  Support: Select a Product: Routers: Cisco 7300 Series Routers

- Cisco 7300 series technical documentation on Cisco.com at

  Support: Select a Product: Routers: Cisco 7300 Series Routers: Install and Upgrade: Install and Upgrade Guides

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2SR and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature modules for Cisco IOS Release 12.2SR are available at the following locations:

- Release 12.2(33)SRA

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122sra33/index.htm

- Release 12.2(33)SRB

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sr/newft/122srb33/index.htm

- Release 12.2(33)SRC

  http://www.cisco.com/en/US/docs/ios/12_2sr/12_2src/12_2_33_src_newfeatlist.html

Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS and Catalyst OS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/cfn

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command reference publications, 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.

- Configuration guides on Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**: **Reference Guides**: **Configuration Guides**

- Command references on Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**: **Configure**: **Command References**

- Configuration guides and command references on http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **Cisco IOS Release 12.2 Configuration Guides and Command References**

Cisco IOS Release 12.2 Documentation Set Contents

Table 1 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in electronic form and in printed form if ordered.

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

On Cisco.com at

Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**

On http://www.cisco.com/univercd/home/index.htm at

Cisco IOS Software: **Release 12.2**

Modules	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Cisco IOS User Interfaces File Management System Management
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2* • *Cisco IOS Bridging and IBM N2etworking Command Reference, Volume 2 of 2*	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSW+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
• *Cisco IOS Dial Technologies Configuration Guide* • *Cisco IOS Dial Technologies Command Reference*	Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Point-to-Point Protocols Dial-on-Demand Routing Dial Backup Dial Related Addressing Service Network Access Solutions Large-Scale Dial Solutions Cost-Control Solutions Internetworking Dial Access Scenarios
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
• *Cisco IOS IP Configuration Guide* • *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services* • *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* • *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*	IP Addressing IP Services IP Routing Protocols IP Multicast
• *Cisco IOS AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk Novell IPX

Modules	Major Topics
• *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide* • *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Cisco IOS Voice, Video, and Fax Configuration Guide* • *Cisco IOS Voice, Video, and Fax Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	ATM Frame Relay SMDS X.25 and LAPB
• *Cisco IOS Mobile Wireless Configuration Guide* • *Cisco IOS Mobile Wireless Command Reference*	General Packet Radio Service

Modules	Major Topics
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Debug Command Reference* • *Cisco IOS Software System Error Messages* • *New Features in 12.2-Based Limited Lifetime Releases* • *New Features in Release 12.2 T* • *Release Notes* (Release note and caveat documentation for 12.2-based releases and various platforms)	

Note *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco.com. From Cisco.com, click the following path: **Support: Software Downloads: Network Management Software: Cisco Network Management Toolkit: Cisco MIBs**.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 1478.

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