Caveats for Cisco IOS Release 12.2(33)SRB through 12.2(33)SRB6

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.)

- Resolved Caveats—Cisco IOS Release 12.2(33)SRB6, page 1048
- Resolved Caveats—Cisco IOS Release 12.2(33)SRB5, page 1073
- Resolved Caveats—Cisco IOS Release 12.2(33)SRB4, page 1093
- Resolved Caveats—Cisco IOS Release 12.2(33)SRB3, page 1113
- Resolved Caveats—Cisco IOS Release 12.2(33)SRB2, page 1183
- Resolved Caveats—Cisco IOS Release 12.2(33)SRB1, page 1239
- Open Caveats—Cisco IOS Release 12.2(33)SRB, page 1277

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

© 2006—2012 Cisco Systems, Inc. All rights reserved.

- Resolved Caveats—Cisco IOS Release 12.2(33)SRB, page 1307

Resolved Caveats—Cisco IOS Release 12.2(33)SRB6

Cisco IOS Release 12.2(33)SRB6 is a rebuild release for Cisco IOS Release 12.2(33)SRB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRB6 but may be open in previous Cisco IOS releases.

- CSCee19691

  Symptoms: A Cisco router may crash when you enter the **clear ip route *** command multiple times.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2S or Release 12.3 and that is configured for RIP.

  Workaround: There is no workaround.

- CSCej05426

  Symptoms: When the standby RP functions in SSO mode and you enter the **no rtr reaction-configuration** *operation-number* command, the standby RP is forced into RPR mode and the active RP cannot enter the configuration mode. The standby RP remains in the initialization mode. You must reload both the active RP and the standby RP to enable them to return into SSO mode.

  Conditions: This symptom is observed on a Cisco 7304 when a probe is created automatically via the IP SLA "rtr mpls-lsp-monitor" commands and when you remove, reschedule, or reconfigure the probe via the **no rtr** *operation-number*, **no rtr reaction-configuration** *operation-number*, or **no rtr schedule** *operation-number* command.

  Workaround: Do not use the CLI to make changes to the probe. Rather, make changes to the probe via the IP SLA "rtr mpls-lsp-monitor" commands.

- CSCek50806

  Symptoms: The standby RP may reload when you enter the **aps revert** command.

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

  Workaround: There is no workaround.

- CSCek77516

  Symptoms: If AToM Tunnel Select feature is used, traffic does not flow.

  Conditions: Occurs with software-based EoMPLS setup, using xconnect under switch virtual interface (SVI).

  Workaround: Use one of the supported physical interface as core-facing line card. Supported line cards include SIP-200, SIP-400, SIP-600, FW2, PWAN2, ES20 and ES40.

- CSCsg00102

  Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

  Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If "debug ip tcp transactions" is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed.

  This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix CSCso04657 and CSCsg00102.

- CSCsg49395

  Symptoms: The following BIT-OUTOFRANGE error message and traceback information may be displayed:

  ```
  1d21h: %BIT-SP-4-OUTOFRANGE: bit 127 is not in the expected range of 128 to 2175
  -Traceback= 40D8A8B0 40D8ADFC 40512B4C 407A8118 40CC5838 404B5978 404B5C84term m
  ```

  Conditions: Occurs on a Catalyst 6500 if an SNMP walker utility sends bridge port number 0 to the switch.

  Workaround: Configure the SNMP walker utility to get MIB objects starting from bridge port number 1.

- CSCsh58542

  Symptoms: Crash seen when the following sequence of commands are configured on an interface:

  1. **ipv6 mld static/join-group** *group* **source-list** *acl1*
  2. **ipv6 mld static/join-group** *group* **source-list** *acl2*

  and then a **shut/no shut** is performed on the interface:

  acl2 is not defined

  Conditions: The problem will be seen when:

  1. Applying the first static-join on one group and the second on another group.
  2. Applying the joins strictly in the above order, such as applying the first static-join with a valid source-list ACL and second static-join on a different group with undefined source-list.

  The problem will not happen if the source-lists are defined on a single-group or all the source-lists are already defined. The problem will be seen only with above conditions when the interface is in the process of "coming-up". In this case, if the interface is up before static-joins, then this particular problem will not be seen until the interface is flipped again.

  Workaround:

  1. Define the source-lists ACLs first before applying the static-joins.
  2. In case, if we have to configure undefined ACLs, apply them first before applying the valid source-list ACL.

- CSCsh85011

  Symptoms: Router crashes.

  Conditions: Occurs during IP SLA operation when the frequency is changed using the **group schedule** command.

  Workaround: There is no workaround.

- CSCsj21099

  Symptoms: IPv4 eBGP session flaps when IPv6 address family is removed from VRF configuration. IPv6 eBGP session flaps when IPv4 address family is removed from VRF configuration.

  Conditions: The problem only happens with Cisco IOS images that support "vrf definition" configuration.

  Workaround: There is no workaround.

- CSCsj34043

  Symptoms: SIP-200 crashes several times due to a memory corruption with the following error messages:

  ```
  Jun 14 16:07:26.239: %OIR-3-CRASH: The module in slot 2 has crashed
  ```

```
Jun 14 16:07:26.239: %OIR-6-REMCARD: Card removed from slot 2, interfaces disabled
[...]
Jun 14 16:07:49.494: %XDR-6-XDRIPCNOTIFY: Message not sent to slot 2/0 (2) because of
IPC error queue flush. Disabling linecard. (Expected during linecard OIR)
Jun 14 16:07:49.474: %OIR-SP-3-PWRCYCLE: Card in module 2, is being power-cycled off
(Module not responding to Keep Alive polling)
Jun 14 16:07:49.494: %C6KPWR-SP-4-DISABLED: power to module in slot 2 set off (Module
not responding to Keep Alive polling)
Jun 14 16:08:29.286: %CWAN_RP-6-CARDRELOAD: Module reloaded on slot 2/0
```

Conditions: Occurs on a SIP-200 running Cisco IOS Release 12.2(33)SRA2 with an OC3 ATM SPA.

Workaround: There is no workaround.

- CSCsk04318

  Symptoms: Under the BGP router configuration mode, removing an address-family configuration and then immediately reapplying the same configuration may cause the standby RP of a dual-RP router to reload unexpectedly. Typically, the following configuration sync error will be reported:

  Config Sync: Line-by-Line sync verifying failure on command: address-family ipv4 vrf NAME due to parser return error

  Removing and replacing the RD configuration under a VRF may also trigger the same type of sync error behavior, although the command listed as failing line-by-line sync will be different.

  Conditions: Removal of a BGP address-family configuration triggers background cleanup processing that occurs asynchronously after the command is entered by the user. The background cleanup runs on both the active RP and the standby RP, although the cleanup may happen at different times on the active and standby. Because such background processing does not usually run in lockstep on the two RPs, a window exists after entering an address-family deconfiguration command where the active RP and standby RP are not in the same state. If the user tries to reconfigure the address-family command before both RPs have completed processing and are again in the same state, line-by-line sync may fail and cause the standby RP to reload.

  Workaround: The line-by-line sync error can be avoided by allowing adequate time for the standby RP to complete background processing and arrive in an identical state as the active RP. If configuration commands are applied when both RPs are in a consistent state, the configuration sync error will not occur and the standby RP will not reload. The background processing normally happens at 60-second intervals, so waiting 2 minutes between deconfig/reconfig attempts for the same command should prevent the issue in all cases.

  The line-by-line sync error and standby RP reload should not cause any service impact, as only the standby RP is affected. The active RP remains fully functional and continues traffic forwarding as usual while the standby RP reloads.

- CSCsk23972

  Symptoms: A router running an IOS image may stop accepting incoming TELNET connections.

  Conditions: Occurs when 20 or more VRFs are configured and they have incoming TCP connections arriving at the host for non-existing services from different VRFs.

  Workaround: Use **show tcp brief all** command to view TCB that have local and foreign addresses as "*.*". Clear those entries using the following command **clear tcp tcb** *address of the TCB*.

  Further Problem Description: When an incoming SYN is received for a non-existing service, for example to BGP port with BGP not configured, TCP leaks a TCB that has laddr and faddr as *.*. This TCB is usually reused for the next incoming connection.

  However when VRFs are configured, such TCB can be reused only for that VRF. If there are several VRFs configured in the box, one TCB per VRF will be leaked. And there is a limit of 20 such "wild TCBs" in the system. So, once we reach the limit of 20, because we leak one per each different VRF, any connection request coming in will be denied.

- CSCsk35970

  Symptom: Excessive CPU usage occurs on a router configured for BGP multipath with several iBGP and eBGP peers.

  Conditions: BGP TblVer is incrementing every 5 minutes, causing the BGP router process to use maximum CPU every 5 minutes.

  Workaround: None

- CSCsk48390

  Symptoms: Tracebacks are seen.

  Condition: Occurs when the T1 corresponding to a member link of a MLPPP bundle is unprovisioned while the link is still part of the bundle.

  Workaround: Remove the member link from the MLPPP bundle and then unprovision the T1.

- CSCsk64158

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

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory.

  This advisory is posted at the following link:

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

- CSCsl32142

  Symptoms: A router may reload after reporting SYS-3-OVERRUN or SYS-3-BADBLOCK error messages. SYS-2-GETBUF with ‘Bad getbuffer’ error may also be reported.

  Condition: Occurs when PIM auto-RP is configured and IP multicast boundary is enabled with the **filter-autorp** option.

  Workaround: Configure IP multicast boundary without the **filter-autorp** option.

- CSCsl57457

  Symptoms: Intermediate System-to-Intermediate System (IS-IS) NSF may not work.

  Conditions: Occurs when router is running a modular Cisco IOS image.

  Workaround: There is no workaround.

- CSCsl58673

  Symptoms: A Cisco router running IOS or IOS Software modularity may not allow telnet connections when the device is configured to run an Embedded Event Manager (EEM) policy that contains actions that use the CLI. In addition CLI actions may not correctly wait for the prompt before going on to the next action or may not detect the prompt.

  Conditions: The symptom of not allowing telnet connections can occur when the device has been configured with an EEM policy to run a CLI command. When that policy exits the input buffer of the VTY way not be cleaned up properly so the next connection opened on that VTY may simply show three user name prompts and exit.

  The symptom of the CLI actions not waiting for the prompt can occur when using the CLI actions on a low-end system with a slower CPU. The system incorrectly checks for the prompt only 10 times and then assumes the prompt is blank instead of waiting for a valid prompt.

The symptom of CLI actions not matching against the prompt properly can occur if the prompt has been changed from the default.

When multiple EEM policies are triggered, they can use up all available VTY lines.

Workaround: There is no workaround.

Further Problem Description: If no VTY lines are available, the user will not be able to Telnet into the machine. Console access will not be affected.

This only affects customers using the Embedded Event Manager (EEM). It affects EEM applets and policies which interact with the CLI library. This was only seen on the MCP platform however.

Cisco IOS Release 12.2(33)SRA is not affected.

Cisco IOS Release 12.2(33)SRB1 and Cisco IOS Release 12.2(33)SRB2 are not affected. But Cisco IOS Release 12.2(33)SRB3 is affected.

Cisco IOS Release 12.2(33)SRC1 is not affected.

Cisco IOS Release 12.2(33)SXF is not affected.

Cisco IOS Release 12.2(33)SXH1 is affected. Cisco IOS Release 12.2(33)SXH2 is not affected.

- CSCsm21126

  Symptoms: A Cisco 7600-SSC-400 may not recover from a fabric error.

  Conditions: The symptom is observed when an error is present in the fabric channel. The fabric errors can be observed by executing the command **show platform hardware** *ssa fabric-monitor history.*

  Workaround: There is no workaround.

- CSCsm27071

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

  * The configured feature may stop accepting new connections or sessions. * The memory of the device may be consumed. * The device may experience prolonged high CPU utilization. * The device may reload.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the “workarounds” section of the advisory.

  The advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml

- CSCsm32392

  Symptoms: A Cisco platform may reset its RP when two simultaneous write memory commands from two different VTY connections are executed.

  Conditions: Occurs on a Cisco 7600 with Sup720. The symptom is intermittent and is related to the way NVRAM is accessed.

  Workaround: There is no workaround.

- CSCsm42477

  Symptoms: Standby reloads with QoS configuration.

  Conditions: Occurs when the active and standby are out of sync.

  Workaround: There is no workaround.

- CSCsm50317

  Symptoms: Service policy counters stop updating after applying a service policy.

  Conditions: The symptom is observed when applying service policy with ACL to virtual template. The policy-map counters become stuck at zero.

  Workaround: Remove the policy and reapply.

- CSCsm93068

  Symptoms: A large number of interfaces (10,000 or more) in a VRF might lead to long boot-up times and CPU hogs.

  Conditions: The symptom is observed if there is a large number of interfaces in a VRF.

  Workaround: There is no workaround.

- CSCso04657

  Symptoms: SSL VPN service stops accepting any new connections.

  Conditions: A device configured for SSL VPN may stop accepting any new SSL VPN connections due to a vulnerability in the processing of new TCP connections for SSL VPN services. If **debug ip tcp transactions** is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed.

  Workaround: There is no workaround.

- CSCso35659

  Symptoms: Layer 3 traffic gets rate-limited to 100pps on toggling xconnect VFI on the VLAN interface.

  Conditions: VLAN (SVI) interface is configured with IP address and routes L3 packets. If xconnect VFI is applied and removed, the traffic rate falls.

  Workaround: Unconfigure and clear the VLAN.

- CSCso42210

  Symptoms: Following reload, controllers come up, but interfaces stay down.

  Conditions: A router with HA Sup720 and non-HA Sup32 is connected with 8xCHT1/E1 SPA, 1xCHSTM1 SPA and 4xCT3 SPA in a SIP-200. Upon reloading 8xCHT1/E1 SPA alone on both sides simultaneously, 6-7 interfaces go down and never come up. They show as up/up in line card but up/down in RP.

  Workaround: There is no workaround.

- CSCso56038

  Symptoms: The following error message may be seen:

  %DUAL-3-INTERNAL: eigrp 4: Internal Error

  Conditions: This symptom is seen when a PE-CE setup using site-of-origin (SoO) tags, in which an PE router that is running EIGRP can learn the same route both by EIGRP (from a CE neighbor) and also by redistribution.

  The above error may be seen when EIGRP on the PE prepares to send information to a neighbor about a route learned from another neighbor (with no SoO tag), but before the information can be sent, the route is replaced by a redistributed route (with an SoO tag). The above error can be seen. This behavior is very dependent on the timing of this series of events.

  Workaround: There is no workaround.

Further Problem Description: It is not clear what functional impact this may have, or whether the error message is purely a warning.

- CSCso56196

  Symptoms: Updates are not being sent or withdrawn.

  Conditions: This symptom occurs when a neighbor flaps an update-group in the process of updating group generation:

  PE1------UUT----PE2

  On UUT there are neighbors PE1 and PE2. If PE1 and PE2 are in same update group, the **show ip bgp all update-group** command will show that.

  Now there are a lot of updates being formatted and sent in the process. The **show ip bgp all replication** command would show the messages which are enqueued for sending out for particular update groups. At this moment, one neighbor goes to idle and is not coming up, then the new updates will not be formatted until the neighbor comes up.

  Workaround: 1) Remove the idle neighbors of the update-group and add again. 2) Clear the IP BGP neighbor that went idle.

- CSCso67195

  Symptoms: Router may crash due to memory corruption:

  ```
  *Apr 7 12:32:14: %SEC-6-IPACCESSLOGRP: list 111 denied pim 0.0.0.0 -> <removed>, 1
  packet
  *Apr 7 12:32:29: %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk
  680A5374 data 680A79A4 chunkmagic FFFFFFFF chunk_freemagic 0 - Process= "Mwheel
  Process", ipl= 0, pid= 274, -Traceback= 0x6169C450 0x60102E78 0x601031E4 0x61D418E4
  0x61D4230C 0x61CF1A48 0x61D1280C 0x61D05FE4 0x61D0E9FC
  chunk_diagnose, code = 1
  chunk name is PIM JP GroupQ
  ```

  Conditions: This symptom occurs when PIM is enabled on an interface and access- list logging is enabled.

  ip pim sparse-dense-mode

  access-list 98 deny any log

  Workaround: Remove access-list logging.

- CSCso71955

  Symptoms: A router running Cisco IOS may experience alignment errors which are generated for every packet received on the serial interfaces and cellular interfaces. A Cisco 7600 Series router or a Cisco 6500 Series router may reload if this occurs when the traffic rate is high on a PA-POS-1OC3 installed in an Enhanced FlexWAN or similar interface.

  Conditions: This is seen when netflow (**ip route-cache flow** or **ip flow ingress**) is configured on a serial interface.

  Workaround: Disable netflow if possible.

  Further Problem Description: A router that shows the alignment error rather than crashing can experience a significant performance impact, as every packet received on the serial interface will need to go through alignment correction.

- CSCso89550

  Symptoms: The router may crash as the rxError on the active slowly increases after every few minutes. The supervisor may have a bad local fabric channel message.

Conditions: The symptoms are observed on a Catalyst 6000 supervisor module that is a SUP720 and is running Cisco IOS Release 12.2(18)SXF12a. There is no user traffic in the system, so the traffic that causes the rxError can only be the heartbeat packet or the diagnostic packet.

Workaround: Disable GOLD diagnostic tool on switches. If the two tests "TestFabricSnakeForward" and "TestFabricSnakeBackward" are disabled from running as HM tests, this issue should not be seen.

- CSCso90058

  Symptoms: MSFC crashes with Red Zone memory corruption.

  Conditions: This problem is seen when processing an Auto-RP packet and NAT is enabled.

  Workaround: There is no workaround.

- CSCsq39180

  Symptoms: Ethernet Connectivity Fault Management (CFM) packets are dropped instead of being forwarded to the Ethernet Virtual Circuit (EVC).

  Conditions: This was observed under normal conditions. An EVC is configured on a SIP-400 with a SPA-5x1GE. The interface is configured for one EVC for a specific VLAN. Coming into that interface was CFM traffic from another switch.

  Workaround: Reload the router.

- CSCsq60016

  Symptoms: A router crashes after a long RSA key string is entered.

  Conditions: This symptom is observed when a very long hex string is entered.

  Workaround: Break the entry into shorter strings.

- CSCsq84670

  Symptoms: ATM OC48 cell packing: No throughput for high traffic over few VCs.

  Conditions: When running packed cell relay over MPLS (PCRoMPLS) with an OC-48 ATM SPA (line rate traffic divided evenly over 2 subinterface PVCs), throughput instantly goes to 0%. Once this occurs, all throughput remains blocked (even for reduced traffic levels) until the SPA is reloaded.

  Workaround: A traffic level of 75% of OC-48 line rate or less divided evenly over two PVCs does not trigger the failure. Also, traffic divided evenly over more than 6 PVCs (even at an aggregate of 100% of line rate) does not trigger the problem.

- CSCsq97167

  Symptoms: IP multicast traffic drops every 100 seconds.

  Conditions: Traffic drops periodically on all output interfaces after stateful switchover (SSO).

  Workaround: There is no workaround.

- CSCsr05746

  Symptoms: ESM20 line card may crash while booting up.

  Conditions: Occurs intermittently with a scaled topology.

  Workaround: There is no workaround.

- CSCsr06707

  Symptoms: When duplicate BGP router-id is received, BGP process does not clear the router-id correctly.

Conditions: Occurs when duplicated BGP router-id is received

Workaround: Enter the **clear ip bgp** command.

- CSCsr17660

  Symptoms: PE-CE performance degradation of 80% on initial convergence.

  Conditions: Occurs when BGP and VPNv4 are configured.

  Workaround: There is no workaround.

  Further Problem Description: Performance is not affected after initial convergence.

- CSCsr18073

  Symptoms: When polling the IP SLA Ethernet MIB, the switch returns an incorrect value for "Destination to Source positive jitter Sum2." Instead, the switch returns the value for "Source to Destination positive jitter Sum2".

  Conditions: The symptom is observed when the IP SLA Ethernet MIB is polled.

  Workaround: There is no workaround.

- CSCsr27794

  Symptoms: BGP does not generate updates for certain peers.

  Conditions: BGP peers show a neighbor version of 0 and their update groups as converged. Out queues for BGP peers are not getting flushed if they have connection resets.

  Workaround: There is no workaround other than entering the **clear ip bgp *** command.

- CSCsr29468

  Cisco IOS Software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

  Cisco has released free software updates that address this vulnerability.

  Several mitigation strategies are outlined in the workarounds section of this advisory.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml

- CSCsr50134

  Symptoms: A DFC or SP module can crash when fast reroute (FRR) is enabled and there are some interface flaps or events that can cause change in FRR primary or backup path.

  Conditions: Occurs when while internal statistics gathering is taking place while one of the following happens:

  * primary path FRR cutover

  * primary path's interface flaps

  * FRR configuration is changed

  Workaround: Avoid FRR configuration changes.

- CSCsr54959

  Symptoms: Router crashed when removing a policy attached to a VLAN interface with a route map and access lists attached.

  Conditions: Occurred on a Catalyst 4500 running Cisco IOS Release 12.2(46)SG. The device may reload unexpectedly due to a software-forced crash. Defect also affects other platforms and releases of Cisco IOS.

Workaround: There is no workaround.

- CSCsr72810

  Symptoms: Unidirectional traffic is dropped when the PBR is configured with “set vrf” option between global and VPN routing/forwarding (VRF).

  Conditions: Occurs under the following scenario:

  - When PBR is configured with “set vrf” option between global and VRF

  - The router is running Cisco IOS Release 12.2(33)SRC1.

  Workaround: Configure the PBR with “set vrf” option among VRFs.

- CSCsr80601

  Symptoms: An ISAKMP SA is not deleted as expected after removing the RSA key.

  Conditions: The issue is seen when the user tries to clear the ISAKMP SAs by issuing the **clear crypto session** command on an IKE SA that has multiple IPSEC SAs.

  Workaround: Use the **clear crypto sa** and **clear crypto is** commands.

- CSCsu36709

  Symptoms: A router may unexpectedly reload.

  Conditions: The symptom is observed specifically with a configuration of Enhanced Interior Gateway Routing Protocol (EIGRP) that is used to redistribute BGP routes. Plain EIGRP is not affected.

  Workaround: Do not use EIGRP to redistribute BGP.

- CSCsu42315

  Symptoms: When the L3VPN prefix uses a tunnel with fast reroute (FRR) protection, there is traffic loss during reoptimization.

  Conditions: Not all prefix in the VRF will observe this issue. This is seen only when there are more than 250,000 prefixes.

  Workaround: There is no workaround.

  Further Problem Description: Traffic loss during re-optimization can be due to faster tunnel cleanup also. It is advisable to configure **mpls traffic-eng reoptimize timers delay cleanup** <*seconds*> to fine tune the cleanup according to the topology.

- CSCsu64215

  Symptoms: Router may incorrectly drop non TCP traffic. TFTP and EIGRP traffic can be impacted as seen in CSCsv89579.

  Conditions: Occurs when the **ip tcp adjust-mss** command is configured on the device.

  Workaround: Disable **ip tcp adjust-mss** on all interfaces. Note that this may cause higher CPU due to fragmentation and reassembly in certain tunnel environments where the command is intended to be used.

- CSCsu67637

  Symptoms: IPv6 address of loopback interface set as passive under Intermediate System-to-Intermediate System (IS-IS) router process is not present in IS-IS database.

  Conditions: Issue is seen when loopback interface is set as passive under router IS-IS configuration and the IPv6 address of the interface is only added afterwards. If the **passive-interface** command is used when the loopback interface already has its IPv6 address configured, issue is not seen.

Workaround: After the IPv6 address is configured under the affected interface, remove and add the passive-interface configuration under the router IS-IS process.

- CSCsu81406

  Symptoms: Following a processor switchover in route processor redundancy (RPR) plus mode, the SM-1CHOC12/T1-SI card on the channelized serial interfaces goes down.

  Conditions: Occurs after the processor switchover in RPR plus mode.

  Workaround: Use **hw-module reset** to solve the issue.

- CSCsu97177

  Symptoms: Device may reload while querying the CISCO-IETF-IP-FORWARD (IPv6) MIB.

  Conditions: SNMP must be configured on the device, and the querier must be aware of the appropriate community to use. Further, there must exist multiple IPv6 global routing tables on the device. This will only be the case if VRFs have been configured with the “vrf definition” command, and that vrf has the IPv6 address family configured, and if that VRF is applied to an interface and global IPv6 addresses configured. This can be confirmed by the existence of multiple tables marked “global” in the output of the “show ipv6 table” command.

  Workaround: Exclude the CISCO-IETF-IP-FORWARD from queries.

  Further problem description: Ensure that SNMP is configured so that it can only be accessed by authorized users.

- CSCsv04674

  Symptoms: The M(andatory)-Bit is not set in Random Vector AVP, which is a must according to RFC2661.

  Conditions: This symptom is observed with Egress ICCN packet with Random Vector AVP during session establishment.

  Workaround: There is no workaround.

- CSCsv04836

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

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

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

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

- CSCsv05934

  Summary: Cisco’s VTP protocol implementation in some versions of Cisco IOS and CatOS may be vulnerable to a DoS attack via a specially crafted VTP packet sent from the local network segment when operating in either server or client VTP mode. When the device receives the specially crafted VTP packet, the switch may crash (and reload/hang). The crafted packet must be received on a switch interface configured to operate as a trunk port.

Workarounds: There are no workarounds available for this vulnerability.

This response is posted at: http://www.cisco.com/warp/public/707/cisco-sr-20081105-vtp.shtml

- CSCsv13243

  Symptoms: Configuring Bidirectional Forwarding Detection (BFD) for a Border Gateway Protocol (BGP) neighbor that is established on a subinterface will cause the BGP session to go down.

  Conditions: Occurs on a Cisco 7600 router with BGP session established on a subinterface and the subinterface is configured in “native vlan” mode while the configured BFD session is in ECHO Mode.

  Workaround: Configure subinterface in “non-native” mode.

- CSCsv14963

  Symptoms: A provider-edge (PE) router configured to run Multicast VPN (MVPN) will not install an alternate MDT next-hop on a route that is learned through an OSPF sham-link.

  Conditions: The symptom is observed when two PEs are configured to run MVPN and create a sham-link between them. Remote routes that are learned through the sham-link will not have an MDT tunnel.

  Workaround: There is no workaround.

- CSCsv16869

  Symptoms: BGP updates may not be sent out.

  Conditions: The symptom is observed when neighbors are flapped in a large- scale scenario.

  Workaround: There is no workaround.

- CSCsv21295

  Symptoms: Due to TestLoopback diagnostic failure on RSP supervisor, the interface is placed to err-disable state.

  Conditions: This is seen when the interface is configured as RJ45 and with speed between 10 to 100mbps.

  Workaround: Configure the speed on RJ45 interface ‘auto’ negotiation and execute the diagnostic test TestLoopback to get the port out of err-disable.

- CSCsv21403

  Symptoms: Traffic is not passed through an Ethernet Virtual Circuit (EVC) service instance.

  Conditions: Occurs after configuring EVC (Ethernet Virtual Circuit) service instance. The **show platform efp-client** command shows no output.

  Workaround: There is no workaround.

- CSCsv22930

  Symptoms: When traffic engineering (TE) and fast reroute (FRR) is configured between the stitching router and provider edge (PE), traffic fails.

  Conditions: Occurs when pseudowire stitching is configured.

  Workaround: Do not enable FRR between these routers.

- CSCsv24179

  Symptoms: Protocol Independent Multicast (PIM) neighborship is not established with SIP600 over R-VPLS.

Conditions: Occurs when more than one VC on different VLANs exists with SIP600 links as core-facing and one of the VLANs configured with PIM.

Workaround: There is no workaround.

- CSCsv24908

  Symptoms: Layer 2 forwarding on other modules breaks when SIP-400 interface running eBGP and GRE flaps

  Conditions: Occurs on a SIP-400 with SPA-2X1GE running BGP and GRE tunnels. Interface flaps on other modules are unable to resolve ARP or maintain routing neighbors. Issue seen on Supervisor 720 and Cisco 6748 CFC ports.

  Workaround: Reload the chassis.

- CSCsv25306

  Symptoms: OSPF between two customer sites over H-VPLS network with SIP600 as core facing card in the hub router fails to come up.

  Conditions: This is seen with traffic engineering (TE) and fast reroute (FRR) TE/FRR setup in the hub, and when TE tunnels have dynamic path option set.

  Workaround: Perform a **shut/no shut** on the core-facing SIP600 interface.

- CSCsv27617

  Symptoms: After reloading, NetFlow stops working and the output of **show ip interface** shows "IP Routed Flow creation is disabled in netflow table"

  Conditions: This condition is seen on WAN main interfaces of a Cisco 7600 running Cisco IOS Release 12.2(33)SRB3 and can also be seen on Cisco IOS Release 12.2(33)SRC2.

  Workaround: Remove and reconfigure NetFlow on the affected interfaces.

- CSCsv28451

  Symptoms: A Cisco 7600 PE router fails to redistribute a VRF prefix into BGP after the prefix or path to it flaps. The PE router will indicate the prefix being redistributed into BGP but the prefix will not get installed into the BGP table until the prefix is cleared:

```
PE2#
PE2#sh ip route vrf foo 10.5.5.5
Routing Table: foo
Routing entry for 10.5.5.5/32
Known via "ospf 1", distance 110, metric 20, type extern 2, forward metric 10
Redistributing via bgp 666
Advertised by bgp 666 metric 10 match internal external 1 & 2
Last update from 10.45.45.2 on Ethernet1/0, 00:00:56 ago
Routing Descriptor Blocks:
* 10.45.45.2, from 10.5.5.5, 00:00:56 ago, via Ethernet1/0
Route metric is 20, traffic share count is 1
PE2#
PE2#sh ip bgp vpnv4 vrf foo 10.5.5.5
% Network not in table
PE2#
```

  Conditions: The PE router redistributing the given prefix must have a sham-link configured for the given VRF and an alternate path to the prefix must exist once the primary (sham-link) is down.

  Workaround: Use the following command: **clear ip route vrf vrfname <prefix>**.

  Further Problem Description: This problem is seen only in Cisco IOS Release 12.2(33)SRB. Cisco IOS Releases 12.2(33)SRC/SRD, etc. are not affected.

- CSCsv29659

Symptoms: RP configured inside a NAT not shown on test device outside the NAT.

Conditions: Entering the **show ip pim rp mapping** command fails to display the RP.

Workaround: There is no workaround.

- CSCsv30307

  Symptoms: ISSU does not work from Cisco IOS Release 12.2(33)SRD to Cisco IOS Release 12.2(33)SRB5.

  Conditions: When ISSU is performed from Cisco IOS Release 12.2(33)SRD image to 12.2(33)SRB5 image, ISSU is not working because of a default command introduced in 12.2(33)SRD.

  Workaround: There is no workaround.

- CSCsv30540

  Symptoms: The error message %SYS-2-CHUNKBOUNDSIB and traceback are seen.

  Conditions: The symptoms are observed when the **show running- config/write memory** command is issued.

  Workaround: There is no workaround.

- CSCsv36266

  Symptoms: E1 and SonetVT layers are down even though serial (Upper Layer) ifOperStatus is UP.

```
Serial1/0/0.1/2/1/1:1 ifOperStatus.156 = up(1)
E1 1/0/0.1/2/1/1 ifOperStatus.157 = lowerLayerDown(7
TU 1/0/0.1/2/1/1 ifOperStatus.158 = down(2)
tug 3-2 tug 2-1 e1-1:chgrp1
AU-4 1, TUG-3 2, TUG-2 1, E1 1 (C-12 1/2/1/1) is up
156 Se1/0/0.1/2/1/1:11500512KUP UP
157 E1 1/0/0.1/2/1/102.05MUP <blank>
158 TU 1/0/0.1/2/1/102.05MUP down
```

  Conditions: Occurs on serial interfaces of SPA-1XCHSTM1/OC3.

  Workaround: There is no workaround.

- CSCsv38166

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

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

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

  Cisco has released free software updates that address this vulnerability.

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

  This advisory is posted at the following link:

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

- CSCsv57587

Symptoms: After online insertion and removal (OIR) of the SPA or line card holding the active Automatic Protection Switching (APS) interface, there are two active interfaces for the same APS group. During OIR, the old inactive interface becomes active and the OIRed interface also comes back up as active. The OIR interface should come up as inactive.

Conditions: The problem is seen only on ATM SPAs and is seen with both SR-APS and MR-APS configurations.

Workaround: In the case of a manual OIR, this can be prevented by entering the **force APS switchover** command before performing an OIR on the active.

When OIR happens due to other reasons and the problem is seen, perform a **shut/no shut** on one of the interface.

- CSCsv73509

  Symptoms: When “no aaa new-model” is configured, authentication happens through the local even when tacacs is configured. This happens for the exec users under vty configuration.

  Conditions: Configure “no aaa new-model”, configure login local under line vty 0 4 and configure login tacacs under line vty 0 4.

  Workaround: There is no workaround.

- CSCsv79673

  Symptoms: Unicast flooding occurs for all traffic destined to VLAN SVI. MAC address for the VLAN SVI is being learned dynamically.

  Conditions: Changing the VLAN SVI configuration from IP to XCONNECT and back without shutting down the interface will result in the router MAC being learned dynamically instead of being installed as static. Normal aging occurs on the dynamic MAC, resulting in unicast flooding if the MAC is removed from the MAC address table.

  Workaround: Perform a **shut/no shut** on the affected VLAN SVI.

- CSCsv79993

  Symptoms: A Cisco 7600 may crash when a distribute-list is deleted.

  Conditions: Crash occurs when removing a distribute-list from EIGRP. The distribute-list was one of many that was sharing the same route-map and access-list. The crash only happens when multiple protocols have the same direction distribute-list configured on the same interface, as in the following example:

  router eigrp 10

  network 10.0.0.0

  distribute-list 49 out Ethernet1/2.10

  router rip

  network 10.0.0.0

  default-metric 2

  distribute-list 49 out Ethernet1/2.10

  Workaround: There is no workaround.

- CSCsv85791

  Symptoms: Traffic out of a Frame Relay subinterface on a Cisco 7600/Enhanced Flexwan/CT3 stops randomly during normal operation. Some traffic is still going through, with delays of 5+ seconds seen using ICMP echo requests with large timeout.

  Conditions: Occurs when an outbound QoS service-policy is configured on the DLCI.

Workaround: Remove the service-policy and re-add it to temporarily restore normal traffic flows.

- CSCsv86256

  Symptoms: In the pseudowire stitching configuration, if fast reroute (FRR) is enabled for link or node protection at the tunnel stitching router, then end-to-end connectivity is broken.

  Conditions: Problem happens only if a Cisco 7600 is the stitching-point router and has MPLS Fast Reroute enabled.

  Workaround: Disable FRR at the stitching point.

- CSCsv97273

  Symptoms: The SP crashes when the device receives an IP address from the DHCP server. The following error message is displayed:

  Signal = 11 Vector = 0x1400

  Conditions: Occurs on a Cisco Catalyst 6500 with RSP720-3C-GE when the **ip verify source vlan dhcp-snooping** is enabled.

  Workaround: There is no workaround.

- CSCsw16698

  Symptoms: New DHCP clients are not able to get IP address from DHCP server via DHCP relay on the router. Existing clients are unable to renew their IP addresses

  Other Symptoms:

  1.1 When we're trying to display DHCP bindings with "show ip dhcp binding" command the following message is observed:

  ```
  % The DHCP database could not be locked. Please retry the command later.
  ```

  1.2 Command "ip dhcp database" disappeared from the running configuration.

  1.3 Output of "show run" is delayed.

  1.4 Output of "debug ip dhcp events" show the following when a new DHCP packet is received:

  ```
  DHCPD: dhcpd_receive_packet: unable to lock semaphore to check for pre-existing
  bindings could not lock se. DHCPD: dhcpd_timer_process could not lock semaphore.
  DHCPD: dhcp_server_receive could not lock semaphore.
  ```

  2.1. This bug may also cause DHCP Snooping failure. In this case, the output of the **show ip dhcp snooping database** command constantly shows these lines:

  ```
  Agent Running : Yes Delay Timer Expiry : 0 (00:00:00) Abort Timer Expiry : Not Running
  ```

  Conditions: Occurs when DHCP and/or DHCP Snooping database agent is configured to store bindings on a TFTP server, and then the database files are not present or are read-only for some time on TFTP server while the router tries to write to them.

  Workaround: Before the issue occurs, there are three known alternatives to avoid this problem:

  1. Either configure "length 0" for line console 0;

  2. Or - log in via console at least once since router startup;

  3. Or - use Cisco IOS Release 12.2(33)SRD but do not enable "debug tftp packet".

  To fix the issue after it has occurred, connect to the router via console, press space bar to get rid of '--More--' prompt, then press enter to log in

- CSCsw24611

  Symptoms: A router configured with BGP and VPN import may crash.

Conditions: This is a hard to hit race condition. BGP imports a path from VRF-A to VRF-B. The following steps have to take place in exactly this order for the crash to occur: 1. The next-hop for the path has to become unreachable. 2. BGP has to re-evaluate the bestpath on the net in VRF-A and result in no-bestpath on the net (because there is no alternative path available). 3. RIB installation has to process the importing BGP net under VRF-B.

Step 3 will result in the crash. If, before step 3, the next-hop re-evaluation manages to process the net in VRF-B then it will clear the bestpath and there will be no crash. If, before step 3, the import code gets a chance to process the net it will clean-up the imported path from VRF-B and then there will be no crash.

Workaround: There is no workaround.

- CSCsw24826

  Symptoms: Cisco router may crash pointing to OSPF code because of low memory access.

  Conditions: Crash is specific to the following scenario:

  1. Neighbor router performs IETF NSF restart.

  2. Software interface between routers is removed from configuration when NSF restart is undergoing, when grace LSA is present in the database of the helper router.

  3. Helper router will crash 1 hour later during max-age procedure for grace LSA. Reason is that grace LSA is associated with interface, but that interface does not exist any more.

  Workaround: If configuration changes need to be done during network changes, the following applies:

  1) Shutdown OSPF interface

  2) Check **show ip ospf da**. Can you see type-9?

  - NO => good, remove interface

  - YES => 'no shutdown' interface, wait for neighbor going FULL (type-9 will be flushed during sync)

  3) Repeat Step 1.

- CSCsw35155

  Symptoms: When using denies in ACLs in crypto maps, the VPN SPA or VPN SM crashes.

  Conditions: Occurs when configuration uses denies in ACLs with crypto maps that causes too many entries in the Ternary Content Addressable Memory (TCAM).

  Workaround: Enter the **crypto ipsec ipv4 deny clear** command.

- CSCsw36872

  Symptoms: VPN-NUM in VLAN-RAM TCAM wrongly provisioned after reconfiguration of Layer 3 port-channel. This changes member link mapping, and VRF membership changes on Layer 3 port-channel. Also discrepancy in L3MGR info between RP and SP for affected port-channel/internal vlan representation observed.

  Conditions: When the command **channel-group <number> mode active** is configured on the member link before the respective Port-channel is configured, this causes the member link interface to go admin down. When the port-channel is configured, the port-channel first comes up and then the member link. This may cause the port-channel to take up the same VLAN which was previously assigned to the member link. If this happens, the symptom is seen.

Workaround: One workaround is to configure the port-channel first and then activate the channel-group on the member link interface. Another workaround is to create a dummy interface so that it takes up the member link's previous VLAN and the port-channel will be assigned a new one, in which case this problem is not seen.

- CSCsw37053

  Symptoms: Traffic with aggregate label was forwarded in wrong VPN, causing the mis-forwarding, as the IP prefix was not present in the VPN routing/forwarding (VRF) table.

  Conditions: Occurs under the following scenario:

  1. Aggregate label should not be using the VPN CAM.

  2. The recirculation VLAN has the wrong VPN number.

  Workaround: Manually correct the wrong **mls vlan-ram entry**.

  Further Problem Description: If there are multiple aggregate labels on a given VRF, there might be a chance of seeing this issue.

- CSCsw43211

  Symptoms: Following errors are seen:

  ```
  %IDMGR-3-INVALID_ID: bad id in id_to_ptr (bad id) (id: 0xFFFFFFFF) -Traceback=
  60476EBC 60477400 60491664 616C5834 616C7EEC 61AB72CC 61AC2E64 61AC2EBC 60FE4274
  60FDEFA4 60FD4180 60FD4874 60FD4BBC 60FD275C 60FD27A0 60FC8F74
  ```

  Conditions: This has been seen on a Cisco 7200 after upgrading to Cisco IOS Release 12.2(33)SRC2.

  Workaround: There is no workaround.

- CSCsw63003

  Symptoms: Memory leak occurs in "BGP Router" process. Memory used by this process increase every day while the number of routes is not increasing.

  Conditions: This occurs on a provider edge (PE) router running Cisco IOS Release 12.2(31)SB or 12.2(33)SB. Problem is seen when VPN routing/forwarding (VRF) is showing important BGP activity.

  Workaround: Reload the router to avoid reaching low memory conditions.

- CSCsw71208

  Symptoms: Cisco 7600 does not respond properly to Link Control Protocol (LCP) echo requests, causing PPP sessions to renegotiate between the router and non-Cisco devices.

  Conditions: Occurs on a Cisco 7600 running Cisco IOS Release 12.2(33)SRC2.

  Workaround: Disable keep-alives on the non-Cisco device.

- CSCsw82462

  Symptoms: A connected prefix from the global routing table has a VPN routing/forwarding (VRF) interface as outgoing interface.

  Conditions: This condition occurs after a **clear ip route x.x.x.x** for the prefix x.x.x.x.

  Workaround: **Shut** the VRF interface, clear the prefix from the routing table, then **no shut** the VRF interface.

- CSCsw88324

  Symptoms: The ESM20G, 7600-ES20-GE3CXL, indicates Major error on show module.

Conditions: No special configuration conditions are needed to reproduce. The online diagnostics status indicates “Major Error”. The major error can be observed following a forced switchover using the **redundancy force-switchover** command.

Workaround: No workaround known. Only reloading the router may cause the ESM20G to recover and pass online diagnostics.

- CSCsw89563

  Symptoms: When there are repeated link flaps on load-balanced paths for TAG to IP or TAG to TAG load balancing, memory leaks may occur.

  Conditions: Occurs when link flaps in PE-CE or P-P or P-PE routers. The leak is proportional to the number of labels in the router.

  Workaround: There is no workaround.

- CSCsw89720

  Symptoms: When we perform SNMP query (getmany) on cbQosPoliceStatsTable and cbQosREDClassStatsTable, CPU utilization reaches 99 % with a single SSH session. If we query cbQosPoliceStatsTable and cbQosREDClassStatsTable from 18 SSH sessions, CPU-HOG error message are seen

  Conditions: Occurs with a large number of policies defined on a GigE subinterface (~4k).

  Workaround: No workaround, other than stopping the query.

- CSCsw93867

  Symptoms: The following messages appear in the log after a reload:

  ```
  Suspending service policy (policyname) on Multilink(#)bandwidth of 24.00% is not
  available (1.00%)
  bandwidth of 24.00% is not available (1.00%)
  bandwidth of 24.00% is not available (1.00%)
  bandwidth of 24.00% is not available (1.00%)
  ```

  Conditions: A Cisco 7600 running Cisco IOS Release 12.2(33)SRB2 and 12.2(33)SRB3 with Multilink interface configured for CBWFQ QOS policy will suspend policy and display error message similar to the above if service-policy is applied to Multilink interface at time of route loading.

  Workaround: Load router with no service-policies applied and apply them after router is up.

- CSCsw98371

  Symptoms: When creating SPAN monitor sessions via SNMP Set (using Network Analysis Module GUI), the user can trigger a high CPU on the supervisor. This then stops the switch from passing traffic and from being accessible.

  Conditions: Occurs under the following scenario:

  1. Cisco 7600 running Sup720 and 12.2(33)SRB or SRC. The 7600 must have a service module (e.g. MWAM module or FWM) that take up a default SPAN reflector monitor session when powered on.

  2. Set up another monitor session. The sup supports no more than two monitor sessions.

  7600#show mon sess all

  Session 1 --------- Type : Service Module Session Modules allowed : 1-9 Modules active : 3 BPDUs allowed : Yes

  Session 2 --------- Type : Local Session Source Ports : Both : Gi9/47 Destination Ports : Gi9/48

  3. When the user attempts to create a new monitor session with the same session number as the “Service Module Session” via SNMP, the creation fails, but breaks the logic to prevent any more SPAN sessions from being created.

4. Hence attempting to create a third monitor session is then allowed, and the High CPU is triggered.

Workaround: 1. Check from the command line if there is a monitor session used by the Service Module using the **show monitor session all** command.

2. If there is, do not attempt to create a new monitor session using the same session number.

OR

3. Create all monitor sessions on the supervisor from the CLI only.

Note: If the Service Module Session is not required, it can be removed with the **no monitor session servicemodule** command.

- CSCsw99846

  Symptoms: With mLDP over a P2P tunnel, traffic drops in multiple cases.

  Conditions: The traffic drops when there is a change in path set entries, which can happen when you perform a **shut** and **no shut** the TE tunnel or toggle MPLS traffic-tunnel or use the **clear mpls traffic-eng auto-tunnel** command.

  Workaround: There is no workaround.

- CSCsx06457

  Symptoms: A router configured with BGP may generate IPRT-3-NDB_STATE_ERROR log messages. An additional symptom when **bgp suppress-inactive** is configured is that the router CPU usage may get close to 100%.

  Conditions: When both BGP and an IGP are advertising the same prefix, the error condition may occur. When in addition **bgp suppress-inactive** is configured high CPU usage by BGP may be seen.

  Workaround: Removing the **bgp suppress-inactive** configuration should eliminate the high CPU problem. Removing either the BGP or IGP conflicting routes from the system should clear both symptoms.

- CSCsx16206

  Symptoms: Incoming traffic destined for Etherchannel is lost due to a configuration error on the ASIC of certain line cards.

  Conditions: Occurs only if Etherchannel is configured across multiple line cards. Chassis contains 6516A and 6548-ge-tx line cards. Etherchannel members do not need to be on the these cards.

  Workaround: Force switching mode to truncated threshold such that it stays in bus mode. Resetting the workaround will fix the line card experiencing the problem, but if the reset causes a switching-mode change from truncated to flow through and back to truncated, then any other line cards with the same ASIC will now experience the problem.

- CSCsx25316

  Symptoms: A device may reload because of a crash after the command **clear ip route *** is executed.

  Conditions: The trigger for this issue is executing the **clear ip route*** command in the presence of a default route. If an RIP update is received by the router while the routing information base is being cleared, the update will be processed causing RIP to check the state of the default route in the routing information base. This combination has the potential to cause a crash.

  The probability of the crash occurring is proportionate to the size of the routing table. The larger the routing table, the greater the chance of encountering the problem.

  Workaround: It is recommended to avoid using the **clear ip route *** command. If the prefix in question is known, then use **clear ip route <prefix>** instead.

Further Problem Description: This problem was observed in Cisco IOS Release 12.2(33)SRC3. All Cisco IOS SR33-based images (SRB, SRC, SRD and SB33) are vulnerable to this problem. The problem will be seen only when using the **clear ip route *** command and is platform independent. Other commands like **clear ip ospf**, **clear ip bgp**, **clear ip isis** or **clear ip route <prefix>** are not vulnerable.

- CSCsx27659

  Symptoms: L3 traffic is blackholed after online insertion and removal (OIR) of Distributed Forwarding Cards (DFCs).

  Conditions: After an OIR, some of the adjacencies (recirculation) may not be correctly programmed when they go online.

  Workaround: Use the **clear adjacency** command to reprogram the adjacencies correctly. This will impact traffic on the router.

  Further Problem Description: Use the **show mls cef adjacency entry <x> detail** command to diagnose. A display of "vlan=0" on recirculation adjacencies indicates this problem.

- CSCsx28948

  Symptoms: Packet leak is observed on Cisco 7200 router running Cisco IOS Release 12.2(33)SRC.

  Conditions: Multicast packet is forwarded to the tunnel interface, causing memory leak. Even packet is dropped, memory leak is observed. Multicast data having less then 64 byte size is dropped at the driver. Leak is not happening with interface other then tunnel interface.

  Workaround: There is no workaround.

- CSCsx33622

  Symptoms: Flapping BGP sessions are seen in the network when a Cisco IOS application sends full-length segments along with TCP options.

  Conditions: This issue is seen only in topologies where a Cisco IOS device is communicating with a non-Cisco-IOS peer or with a Cisco IOS device on which this defect has been fixed. The router with the fixed Cisco IOS software must advertise a lower maximum segment size (MSS) than the non-fixed Cisco IOS device. ICMP unreachables toward the non-fixed Cisco IOS router must be turned off, and TCP options (for example, MD5 authentication) and the **ip tcp path-mtu-discovery** command must be turned on.

  Workaround: Any value lower than the advertised MSS from the peer should always work.

  Setting the MSS to a slightly lower value (-20 to -40) is sufficient to avoid the issue. This number actually accounts for the length of TCP options present in each segment. The maximum length of TCP option bytes is 40.

  If the customer is using MD5, Timestamp, and SACK, the current MSS should be decreased by 40 bytes. However, if the customer is using only MD5, the current MSS should be decreased by 20 bytes. This should be enough to avoid the problem. For example:

  1. If the current MSS of the session is 1460, New MSS = 1460 - 40 = 1420 (accounts for maximum TCP option bytes; recommended).
  2. If the current MSS of the session is 1460, New MSS = 1460 - 20 = 1440 (accounts for only the MD5 option).

- CSCsx37313

  Symptoms: When using encapsulation PPP on a POS SPA OC192POS-XFP in a SIP-600, the protocol comes up on both sides and IP Control Protocol (IPCP) is open for PPP. Pinging the remote side fails due to corruption of the PPP frame.

  Conditions: Occurs when using encapsulation PPP on a POS SPA OC192POS-XFP

Workaround: Use High-Level Data Link Control (HDLC) encapsulation.

- CSCsx37431

  Symptoms: CE-to-CE ping for packet size less than 48 bytes fails or applications like telnet fail.

  Conditions: Occurs with ATM SPA on SIP200. ATM PA on FW2 should be one of the CEs facing, while other PEe should be 7200

  Workaround: There is no workaround.

- CSCsx47554

  Symptoms: With a topology like this:

  CE | type 4 xconnect type 4 xconnect |---------- 7600 ---------- GSR ---------- CE SIP400 Sup720 Giga subif Giga subif

  the packets above 1496 are not passing through end-to-end.

  The MTU on the edge-facing interfaces is 1500, the one on the core-facing interfaces is 1600.

  Conditions: The GSR on the other side seems not to have a similar behavior. The bug has been reproduced in Cisco IOS Release 12.2(33)SRB3 and SRC3.

  Workaround: Increase the MTU on the edge-facing interface end-to-end

- CSCsx57465

  Symptoms: On a Cisco 7600-SIP-200 / SPA-2XOC3-ATM running the c7600s72033-adventerprisek9-mz.122-33.SRB4 image, an ATM interface may suddenly cease processing ingress packets resulting in all VC sharing the physical interface being shut down.

  Conditions: Occurs when the ATM SPA interface is configured for LFI.

  Workaround: There is no workaround.

- CSCsx76308

  Symptoms: Cisco 6500 crashes with Breakpoint exception, CPU signal 23.

  Conditions: An attempt to free unassigned memory is seen before the crash:

  ```
  00:01:25: %SYS-2-FREEFREE: Attempted to free unassigned memory at 50D9D260, alloc
  40CC9960, dealloc 40CC9A90
  -Traceback= 41044F88 40CC9A98 40CC88C0 40CC20E4 40CCF5B0 406AF1AC 4069A834 4101848C
  41018478
  ```

  Workaround: There is no workaround.

- CSCsx79111

  Symptoms: MPLS packets that need a swap label may get punted to CPU because the outgoing interface/label has wrong MTU value in hardware (MLS). Once the packet is punted to CPU, it is forwarded correctly, as Cisco Express Forwarding (CEF) in software has correct info. If the traffic rate is high, this causes high CPU.

  -**show mls status** can confirm the MTU failure increasing.

  -**remote command switch show mpls platform vlan** shows wrong MTU for outgoing interface.

  -**show mls cef mpls label X detail** will show the MTU as 0.

  -**show mpls forwarding-table interface X detail** shows good MRU value.

  Conditions: Occurs on a Cisco 7600 running Cisco IOS Release 12.2(33)SRB5.

  Workaround: Re-stating the **mtu** command or **mpls ldp mtu ...** does not make any difference. You need to either bounce the affected interface or reload the switch.

- CSCsx82880

Symptoms: MAC security on ESM20 ports stop working after unrelated configuration changes are done to any other ports on the same ESM20.

Conditions: On ESM20 ports having service instances configured with MAC security on them, traffic stops flowing on those EVCs when unrelated configuration changes are done on other ports on that ESM20.

Workaround: Perform a **shut/no shut** on the affected port.

- CSCsy07555

  Cisco IOS devices that are configured for Internet Key Exchange (IKE) protocol and certificate based authentication are vulnerable to a resource exhaustion attack. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 security associations (SA) and prevent the establishment of new IPsec sessions.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-ipsec.shtml

- CSCsy10610

  Symptoms: LACP L3 POCH members flap, getting unbundled and bundled back again.

  Conditions: Global native VLAN tagging has to be enabled, and L3 POCH interface should have a sub-interface configured under it.

  Workaround: Disable global VLAN tagging.

- CSCsy26883

  Symptoms: VPN routing/forwarding (VRF) traffic may experience packet loss after a supervisor switchover.

  Conditions: Occurs on a Cisco 7600 running Cisco IOS Release 12.2(33)SRB2 or Cisco IOS Release 12.2(33)SRC2.

  Workaround: Apply an access-list with “permit ip any any” in one of the VRF interfaces, or force another switchover.

- CSCsy27500

  Symptoms: Router ID change results in the following error message:

  %BGP-3-NOTIFICATION: sent to neighbor 1::1 passive 2/3 (BGP identifier wrong) 4 bytes 01000003

  Conditions: Occurs after changing BPG router ID in a router running a release of Cisco IOS in which CSCsv20276 is a resolved defect.

  Workaround: Enter the **clear ip bgp** command.

- CSCsy29534

  Symptoms: In rare conditions, when removing address-family in router RIP configuration just after importing large amount of routes in it, the router may crash on bus error.

  Conditions: It was observed in the following context:

  1) Supervisor 720 running Cisco IOS Release 12.2(18)SXF7. 2) 66K of routes were imported at that moment from BGP into RIP. 3) The address-family is removed.

  Workaround: Wait a few minutes between the moment you create and import the routes in the address-family and the moment you remove it. Typically 3-5 minutes (depending on the number of routes, more delay may be needed).

- CSCsy58115

Symptoms: In a router running BGP, the BGP process may hold increased amounts of memory over time without freeing any memory. This may also be seen from the output of **show proc mem sort** and in the output of **show ip bgp sum** or **show ip bgp vpnv4 all sum** and looking at the number of BGP attributes which may be increasing over time in relation to the BGP prefixes and paths which may remain roughly the same.

Conditions: Some BGP neighbors are not in established state and exchanging prefixes. The issue is observed on all platforms running the following releases of Cisco IOS:

-12.2(31)SB14

-12.2(33)SB1b

-12.2(33)SB2

-12.2(33.05.14)SRB

-12.2(33.02.09)SRC

-12.2(33)SRC3

-12.4(20)T2

-12.4(22)T1

-12.2(33)SXI or later releases.

Workaround: Remove the configuration lines related to the inactive neighbors (neighbors in Idle or Active states).

- CSCsy71343

  Symptoms: Flood of broadcast or multicast traffic on Virtual Private LAN Services (VPLS) VCs stops if the path changes from one interface to another interface.

  Conditions: Cisco 7600 provider edge (PE) router running Cisco IOS Release 12.2(33)SRB and using ESM20 as the core-facing links providing multiple paths to reach the VC destination. Cisco IOS Release 12.2(33)SRC and 12.2(33)SRD are not affected.

  Workaround: Choose one of the following options: 1) Perform a **shut/no shut** on the switch virtual interface (SVI).

  2) Remove and add the neighbor from VFI on which the problem is seen.

- CSCsy83830

  Symptoms: Router crashes when we send multiple access packets for same username when configured for RADIUS Load Balancing (RLB).

  Conditions: Occurs with the following topology

  CLIENT----->RLB----->SERVER

  Client sends multiple access retry packets to server and router crashes after a period of time. This issue will be seen in cases where multiple access requests are seen for the same username, and 60 seconds expire since the arrival of the first of such access requests, before an accounting start for the same username is seen.

  Workaround: If RLB do not see multiple access packets we wouldn't see any crash.

- CSCsy87385

  Symptoms: For IPv6 adjacencies, MTU is incorrectly programmed.

  Conditions: Occurs with simple IPv6/6PE setup.

  Workaround: There is no workaround.

- CSCsz10073

Symptoms: SPA-4XOC3-ATM can stop forwarding ingress traffic after cell packing timer is changed.

Conditions: Occurs when MPLS is configured over a tunnel interface and the cell packing timer is changed.

Workaround: There is no preventive workaround to this issue. Once the card is in the problem state, the FPGA is hung and to recover from this state, the SPA has to be reloaded.

- CSCsz19323

  Symptoms: Unable to create monitoring sessions using network analysis module (NAM) graphical user interface (GUI).

  Conditions: Occurs when SNMPSet is used to create the sessions using portCopyTable.

  Workaround: There is no workaround.

- CSCsz45226

  Symptoms: Multicast Open Shortest Path First (OSPF) Bidirectional Forwarding Detection (BFD) packets are corrupted when going out of ESM20 interface on an Ethernet Over MPLS (EoMPLS) setup.

  Conditions: When sending a multicast OSPF database descriptor (DBD) packets or multicast ping packets to the 224.0.0.5 address and the packet size grows above a certain size (108B) in the payload, a specific byte of multicast packet traversing the EoMPLS link is corrupted.

  Workaround: There is no workaround.

- CSCsz45509

  Symptoms: Dead Peer Detection (DPD) packets are not sent following loss of ISAKMP SA and IPSec in UP-NO-IKE state.

  Conditions: Occurs when DPD is configured and ISAKMP SA is deleted independently of IPSec SAs

  Workaround: Manually clear the crypto session to create a new ISAKMP SA.

- CSCsz47619

  Symptoms: ES-20 line card repeatedly resets.

  Conditions: Occurs when fabric sync failure occurs on ES-20.

  Workaround: Enter the following command: **test scp linecard keepalive disable**.

- CSCsz63442

  Symptoms: Router crashes.

  Conditions: This issue is observed on a Cisco 7200 router running an internal build of Cisco IOS Release 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCsz72581

  Symptoms: Dead Peer Detection (DPD) does not trigger a new IKE session if the previous IKE session fails.

  Conditions: Occurs when using on-demand DPD.

  Workaround: Manually clear the IKE session to trigger a new IKE.

Resolved Caveats—Cisco IOS Release 12.2(33)SRB5

Cisco IOS Release 12.2(33)SRB5 is a rebuild release for Cisco IOS Release 12.2(33)SRB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRB5 but may be open in previous Cisco IOS releases.

- CSCec72958

  Symptoms: A Cisco router that is configured for Network Address Translation (NAT) may reload unexpectedly because of a software condition.

  Conditions: This symptom can occur when the router translates a Lightweight Directory Access Protocol (LDAP) packet. NAT translates the embedded address inside the LDAP packet. This problem is strictly tied to NAT and LDAP only.

  Workaround: There is no workaround.

- CSCeg86665

  Symptoms: DSCP value is not being preserved when the ingress packet is encapsulated with a GRE header. The DSCP value will be rewritten to 0 as the packet egresses the router.

  Conditions: The router must be a tunnel endpoint and packets must be marked for this behavior to trigger.

  Workaround: Configuring the **mls qos marking ignore port-trust** command will cause egress packets to be marked correctly.

- CSCek55562

  Symptoms: A CPUHOG may occur.

  Conditions: This symptom is observed with various routing commands, including the **clear ip route** command, in cases where more than 300,000 routes were learned via a single subnet.

  Workaround: There is no workaround.

- CSCek78031

  Symptoms: Some BGP routes are missing from RIB so packets cannot reach the destination.

  Conditions: A connected route covers the BGP route in question, but the connected route is less specific than some other route that is also in the RIB. It leads to BGP to have some prefixes' nexthops inaccessible, and those prefixes are not installed in to RIB, therefore traffic is stopped.

  Workaround: There is no workaround.

- CSCek79227

  Symptoms: Multilink Point-to-Point Protocol (MLPPP) interfaces across Channelized SPA T1s may continuously flap.

  Conditions: Occurs after repeatedly triggering **shut/no shut** on the MLPPP interfaces.

  Workaround: Disable keep-alives across the MLPPP interfaces.

- CSCsb03401

  Symptoms: You cannot open a specific port on a Cisco IOS IP SLA responder.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(14)T1 when you attempt to open a specific port on the responder instead of using normal control protocol. The symptom may also occur in Release 12.4 or Release 12.4T.

  Workaround: Use normal control protocol.

- CSCsc97727

Symptoms: An access point may crash when you add or remove TACACS servers via the CLI.

Conditions: This symptom is observed on a Cisco router that has **aaa accounting commands** *level* **default** *list-name* **group** *groupname* command enabled.

Workaround: Disable the **aaa accounting commands** *level* **default** *list-name* **group** *groupname* command.

- CSCsg11616

  Symptoms: While restarting the iprouting process, the system crashed at redzone corruption.

  Conditions: Occurs following a switchover. The iprouting process should restart once the standby becomes active.

  Workaround: There is no workaround.

- CSCsg27783

  Symptoms: When an SVI is configured with VLAN ACL and Reflexive ACL and then an ingress policy-map is applied on the same SVI, SP TCAM in ingress is programmed correctly but DFC TCAM is programmed incorrectly.

  Conditions: The symptoms are observed on a Cisco Catalyst 6000 Series Switch, or a Cisco 7600 series router that is running Cisco IOS Release 12.2SX, Release 12.2(33)SX, Release 12.2SR or Release 12.2(33)SR and that has a DFC line card.

  Workaround: Entering the **shutdown** command on the VLAN followed by the **no shutdown** will bring the VLAN to the correct state.

- CSCsg39754

  Symptoms: When DHCP snooping is configured on a VLAN, the redirect access list programmed in TCAM permits a wide range of UDP ports from bootps/bootpc to 65xxx.

  Conditions: UDP traffic to these destination ports (0x143, 0x243, 0xFF43) is being redirected to Route Processor (RP). If "ip dhcp snooping limit" is not configured, then RP CPU goes to 100%.

  Workaround: There is no workaround.

- CSCsh20497

  Symptoms: Configuring EIGRP IPv6 may under certain circumstances cause the router to unexpectedly restart.

  Conditions: This issue only applies to a configuration with EIGRP IPv6 configured on serial interfaces, such as Frame Relay hub and spoke or point-to-point serial interfaces. This problem does not affect LAN interfaces or those that use EIGRP IPv4.

  Workaround: There is no workaround.

- CSCsh48879

  Symptoms: A vulnerability exists in the Cisco IOS software implementation of Layer 2 Tunneling Protocol (L2TP), which affects limited Cisco IOS software releases.

  Several features enable the L2TP mgmt daemon process within Cisco IOS software, including but not limited to Layer 2 virtual private networks (L2VPN), Layer 2 Tunnel Protocol Version 3 (L2TPv3), Stack Group Bidding Protocol (SGBP) and Cisco Virtual Private Dial-Up Networks (VPDN). Once this process is enabled the device is vulnerable.

  This vulnerability will result in a reload of the device when processing a specially crafted L2TP packet.

  Cisco has released free software updates that address this vulnerability.

Workarounds that mitigate this vulnerability are available in the "workarounds" section of the advisory.

The advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-l2tp.shtml

- CSCsh48947

  Symptoms: Some of the 48 power over Ethernet ports of a line card cannot be configured as "power inline static" with the maximum power capacity, 15.4 watts, that a port can support.

  Conditions: The number of supported ports depends on the power rating of the voice daughter board. One or more ports may not operate at maximum capacity.

  Workaround: There is no workaround.

- CSCsh66978

  Symptoms: On Cisco 7600 routers, configuring a Switch Virtual Interface (SVI) with VRF may result in traffic on the VRF being dropped.

  Conditions: This is a race condition at configuration time, so if VRF traffic works after the interfaces have been configured, then the problem is not present. Performing a **shut/no shut**" on the VLAN or base interface and/or **switchport/no switchport** on the base interface may cause the problem to appear.

  This is fixed in Cisco IOS Release 12.2(33)SRC and later releases.

  Workaround: Disable and re-enable switchport on the base interface. Also, **shut/no shut** the VLAN or base interface may cause the VRF traffic to pass again.

- CSCsh91889

  Symptoms: BGP session failed to establish between two multicast VPN peers.

  Conditions: Occurs when one peer is configured using new **MDT SAFI BGP** command and the next peer is configured using older **MDT VPNv4** command.

  Workaround: There is no workaround.

- CSCsi82337

  Symptoms: Packets are not switched by Cisco Express Forwarding (CEF).

  Conditions: Occurs under the default condition when **ip cef** is enabled, and packets are neither CEF- or process-switched.

  Workaround: There is no workaround.

- CSCsj19808

  Symptoms: When the gateway for a default route is removed from the routing table, the default route is not removed and the following log message is seen:

  ```
  00:04:35: %IPRT-3-RIB_LOOP: Resolution loop formed by routes in RIB
  ```

  Conditions: A default route resolves on a non-recursive gateway, such as a gateway covered by a directly connected prefix. The interface transitions to down state and the connected route is removed. The default route should be removed from the RIB, but it is not.

  Workaround: If the default route is a static route, then the configuration can be deleted and added again, which will correct the problem. For example:

  no ip route 0.0.0.0 0.0.0.0 10.1.1.1

  ip route 0.0.0.0 0.0.0.0 10.1.1.1

- CSCsj36133

Symptoms: A BGP neighbor may send a notification reporting that it received an invalid BGP message with a length of 4097 or 4098 bytes.

Conditions: The problem can be seen for pure IPv4 BGP sessions (no MP-BGP in use) when the router that is running the affected software generates a large number of withdraws in a short time period and fills an entire BGP update message (up to 4096 bytes normally) completely with withdraws. Because of a counting error, the router that is running the affected software can generate an update message that is 1 or 2 bytes too large when formatting withdraws close to the 4096 size boundary.

Workaround: The issue is not seen when multiple address families are being exchanged between BGP neighbors.

- CSCsj46607

  Symptoms: On Cisco 7600 routers, configuring Unicast Reverse Path Forwarding (Unicast RPF) for prefixes that are reachable via multiple paths may not set unicast RPF correctly on all paths.

  Conditions: If unicast RPF is enabled on the first path, it will show up as being enabled on all paths in **show mls cef ip** <*prefix*>. If it is enabled on the first path and the unicast RPF configuration of other paths is changed, the unicast RPF for the prefix is not updated.

  Workaround: There is no workaround.

- CSCsj49293

  Symptoms: The interface output rate (214 Mb/s) is greater than the interface line rate (155 Mb/s).

  Conditions: This symptom is observed with a Cisco 7600/7500/7200-NPE400 and below. That is, PA-POS-2OC3/1OC3 (PULL mode).

  Workaround: There is no workaround.

  Further Problem Description: From the Ixia, packets are transmitted at 320 Mb/s. On the UUT (Cisco 7600), the outgoing interface (POS-Enhanced Flexwan) shows the output rate as 200 Mb/s. But the interface bandwidth is 155 Mb/s.

- 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, etc.

  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.

- CSCsj90682

  Symptoms: The number of packets that are queued inside a BW queue is more than its displayed queue-limit. In the output for **show policy-map interface**, you see that the child shaping class is buffering to a greater value than its displayed queue-limit.

  Conditions: Occurs when HQOS policy map is applied on an EVC under ESM20 interface.

  Workaround: There is no workaround.

- CSCsj94583

  Symptoms: When a service policy with “priority + Police cir percent x” is applied on a subinterface, it is not getting accepted for all of the percent values.

Conditions: When “police cir percent” conversion to cir value increases a certain range the policy is not getting accepted.

Workaround: There is no workaround.

- CSCsj98198

  Symptoms: The following error occurs:

  ```
  %NETFLOW_AGGREGATION-4-OER_AGG_EXPORT_ERROR: OER Error receiving TT agg export packet
  on RP
  ```

  Conditions: Errors may be seen on Cisco 6500 running as Optimized Edge Routing (OER) border router

  Workaround: There is no workaround.

- CSCsk09471

  Symptoms: Multiple spurious fabric CRC error messages may be displayed on the console.

  Conditions: Caused by incorrect handling of fabric CRC errors. This may result in spurious messages being printed and also results in unnecessary fabric re-sync.

  Workaround: There is no workaround.

- CSCsk28361

  Symptoms: 4000 virtual-template (VT) takes high CPU during system load configuration.

  Conditions: Occurs when 4000 VT interfaces are loaded from TFTP to running configuration.

  Workaround: There is no workaround.

- CSCsk48366

  Symptoms: The following traceback occurs following a stateful switchover (SSO).

  CWAN_SPA-3-POWER_CYCLE: Configuration mismatch occurred on Shared Port Adapter 2/0

  Conditions: Occurred on a Cisco 7600 router running Cisco IOS Release 12.2SRB image with 8T1E1-SPA.

  Workaround: There is no workaround.

- CSCsk63794

  Symptoms: Crash may happen under regular operations as well as when changes to QoS policies are being made.

  Conditions: Occurs on a Cisco 7600 with enhanced FlexWAN module and PA-2T3+ with about 70 frame-relay PVCs in point-to-point topology.

  Workaround: Shut the interface instance before applying/removing the policy.

- CSCsk72676

  Symptoms: PVC does not come up after removing vc-class from it.

  Conditions: This issue happens only when vc-class with constant bit rate (CBR) is configured on the main interface, and another vc-class is applied to the VC. This occurs under the following scenario:

  1.Boot the router afresh.

  2.Apply a vc-class (class1) to the ATM interface.

  3.Configure PVCs with the range command.

  4.Apply another vc-class (class2) under the range-pvc configuration.

  5.Remove the vc-class (class2) from under the range-pvc configuration.

After this step the PVCs are expected to come up having attributes of vc-class class1. The PVCs do not come up and stay in inactive mode.

Workaround: There is no workaround.

- CSCsk84925

  Symptoms: Platforms, such as the Cisco Catalyst 6500, are capable of dropping multicast traffic in hardware. However, in order to do so, they require that mroute entries be created by software. In the case of SSM mroutes on a first-hop router, software does not always create such entries and so this traffic cannot be dropped in hardware, resulting in high CPU utilization on the route-processor.

  Conditions: This symptom will be encountered in the following scenario:

  1. There are no receivers present for a given SSM (S,G) flow 2. (S1,G) has already been created 3. A directly-connected source (S2,G) starts sending traffic

  That is, the first flow (S1,G) will be created and will be properly dropped in hardware if no receivers for that flow are present. Subsequent flows to the same group G will not be created and will impact the route-processor CPU.

  Workaround: There are several possible workarounds to this issue:

  1. Disable the mroute-cache on the incoming interface using the interface-mode command **no ip mroute-cache**. On platforms such as the Catalyst 6500, this will have no impact for hardware-switched flows.

  2. Ensure that all SSM source traffic is sent to unique groups.

  3. Ensure that receivers are present for all anticipated traffic.

- CSCsk86381

  Symptoms: Memory leak occurs in "Crypto IKMP" and "IPSEC key engine"

  Conditions: Occurs on a WS-C6509-E running internal image s72033-advipservicesk9_wan-mz.NAT-D- 5

  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 SIP-400-SPA corrects the problem.

  2) A **shut/no shut** on the protect interface corrects the problem.

- CSCsk88760

  Symptoms: The system crashes when configuration on the member ports of Layer-2 port-channel is changed.

  Conditions: This happens mainly, when members are changed from **switchport** to **no switchport**, while LACP port-channel is established and LACP control packets are being exchanged between the peers. This situation rarely occurs.

  Workaround: There is no workaround.

- CSCsk98751

  Symptoms: A router may crash after the command **mpls traffic-eng backup-path tunnel** is issued.

Conditions: The symptom is observed when a backup tunnel is configured on PLR, which is a mid point router for a protected primary tunnel.

Workaround: There is no workaround.

- CSCsl07297

  Symptoms: Router may crash when a sequence of commands are executed in quick succession.

  Conditions: Occurs when a Border Gateway Protocol (BGP) neighbor belongs to a particular peer group and the following commands are entered in quick succession: * **no neighbor a.b.c.d peer-group pgroup-name** * **no neighbor a.b.c.d description xyz** If these commands executed quickly, such as when they are pasted into the interface, the router may crash.

  Workaround: Use the **no neighbor a.b.c.d peer-group pgroup-name** command to remove the neighbor. This command removes the neighbor and eliminates the need for the second command.

- CSCsl21123

  Symptoms: Entering the **dir stby-harddisk:** command causes the active RP to reload.

  Conditions: Occurs on a Cisco 7600 router.

  Workaround: There is no workaround.

- CSCsl28278

  Symptoms: Routes and packets are lost.

  Conditions: Occurs because NSF restart is not recognized by some of the neighbors after a router restarts.

  Workaround: There is no workaround.

- CSCsl32122

  Symptoms: VPN client users using a certificate to connect to a Catalyst 6000 or Cisco 7600 with VPN blade fail to connect. IPSec negotiation fails during mode configuration.

  Conditions: Conditions are unknown at this time.

  Workaround: Preshared key authenticated VPN clients can connect without problem.

- CSCsl50471

  Symptoms: Egress traffic stops on AToM Cell Relay shaped VC configured on an OC3 SPA interface when the received load from the MPLS network exceeds the egress shaped rate.

  Conditions: An AToM Cell Relay shaped VC is configured on an OC3 SPA interface in a SIP-400. The received load from the MPLS network exceeds the egress shaped rate.

  Workaround: Configure an ingress MQC service policy to police the ingress traffic rate.

- CSCsl62963

  Symptoms: Router crashed while reconfiguring a three-level policy.

  Conditions: Seen on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsl65047

  Symptoms: Back-to-back ping fails after configuring "native" on subinterface.

  Conditions: Initially ping works fine, but packets go out tagged, which should not be the case. On doing a **shut/no shut** on one sub-interface with native configured cause ping to fail since the side that was flapped starts sending untagged ping packets (which is the expected behavior). The remote side that has not been flapped, expects tagged packets.

Workaround: Do **shut/no shut** on both ends of the sub-interface.

- CSCsl92316

  Symptoms: Router may experience mwheel CPUHOG condition.

  Conditions: This condition is observed on Cisco router while clearing all L2TP sessions when there are more than 2500 sessions with multicast traffic flowing on the sessions.

  Workaround: There is no workaround.

- CSCsl99156

  Symptoms:

  1. The No_Global bit (0x10) for MOI flag is incorrectly set for iBGP when it becomes best path.

  ```
  router#show ip cef vrf <vrf name> x.x.x.x int [snip] MPLS short path extensions: MOI
  flags = 0x16 <-------MOI flags 0x10 is incorrectly set for iBGP when it becomes best
  path, correct flag should be 0x4, 0x5, 0x6 ... correct now.
  ```

  2. The No_Global bit (0x10) for MOI flag for iBGP path was incorrectly unset when eBGP becomes best path.

  ```
  router#show ip cef vrf <vrf name> x.x.x.x int [snip] MPLS short path extensions: MOI
  flags = 0x5 <-------MOI flags 0x10 is incorrectly clear for ibgp path when eBGP
  becomes best path, correct flag should be 0x14, 0x15, 0x16... correct now.
  ```

  Conditions: This symptom sometimes happens after BGP path update.

  Workaround: Issue the **clear ip route vrf** *vrf name* **x.x.x.x/y** command.

- CSCsm01389

  Symptoms: Crash occurs after clearing auto-tunnel backup by issuing the **clear mpls traf-eng auto-tunnel backup** command.

  Conditions: Occurs with SSO and traffic engineering (TE) auto-tunnel feature enabled.

  Workaround: There is no workaround.

  Further Problem Description: Crash was seen on Active SP after issuing **clear mpls tra auto-tunnel primary** followed by **clear mpls tra auto-tunnel backup** command. This crash could happen with or without a SSO switchover before issuing those commands.

- CSCsm15350

  Symptoms: The VPNSPA may crash with an assert failure.

  Conditions: The symptom is observed when B2B is configured and when creating 8000 remote access sessions.

  Workaround: There is no workaround.

- CSCsm20599

  Symptoms: A line-by-line synchronization failure may occur and the standby RP may be reset.

  Conditions: The symptoms are observed when a PVC is created on a P2P sub- interface, and when "exit" or "end" is not called.

  Workaround: After creating a PVC on a P2P sub-interface, call "exit" or "end".

- CSCsm28287

  Symptoms: After shutting down a GRE tunnel interface, the active RP crashed and switchover took place.

  Conditions: Occurred on a Catalyst 6000 running an internal build of Cisco IOS Release 12.2SX. Other versions of Cisco IOS Release 12.2S are also affected.

  Workaround: There is no workaround.

- CSCsm40666

  Symptoms: Using the **execute-on** command on SUP to PPC may cause the device to hang in some cases.

  Conditions: This happened when the SUP process is busy with CLI process, including the case where CLI-intensive management application is running.

  Workaround: Open another Telnet session enter the same **execute-on** command. This will release the first hung **execute-on**.

- CSCsm50741

  Symptoms: When a non-DC router is removed from a DC enabled area and the area becomes DC enabled, some of the LSAs are not refreshed correctly with DoNotAge (DNA) bits set. Crash may happen when customer deploys iptivia probes in the network. Fixed in CRS.

  Conditions: The symptom is observed when a router without DC capability is removed from a DC enabled area.

  Workaround: Use the **clear ip ospf** command.

- CSCsm53196

  Symptoms: Crash occurs at “ip_route_delete_common”.

  Conditions: Occurs under the following scenario:

  1)A multicast BGP route exists.

  2)A unicast BGP route exists for the same prefix.

  3)Another route covered by the same majornet as the BGP route exists.

  4)There are both iBGP and eBGP sources for the BGP prefix.

  5)Redistribution of BGP routes into an IGP must be configured.

  Topology change in network causes mBGP to switch from using the iBGP sourced route to the eBGP sourced route will cause the crash.

  Workaround: If there are not both iBGP and eBGP sources for the same route the problem will not occur. If redistribution of BGP Into an IGP is not configured the problem will not occur.

- CSCsm55817

  Symptoms: When configuring ATM PVCs, under the PVC syntax you can provide a handle to describe the PVC. If this handle starts with “00” (zero zero) then the command will fail.

  Conditions: The symptom is observed when configuring ATM PVCs and where the PVC handle starts with "00".

  Workaround: Do not use handles that start with "00".

- CSCsm57494

  Symptoms: BGP update is not sent after reloading opposite router or resetting module. Sometimes a BGP VPNv4 label mismatch also occurs between the routers because BGP update is not received.

  Conditions: - This problem may occur once or twice out of 20 attempts. - This problem is apt to occur when MPLS-TE tunnel is enabled. - This problem may occur when entering either **reload** command, **hw-module module X reset** command or the **clear ip bgp X.X.X.X** command on the opposite router.

  Workaround: There is no workaround.

- CSCsm61571

Symptoms: When the optical RX level changes such that is out of the supported threshold or a mismatched combination of XFPs used at ends (eg: ZR to LR, SR to LR, etc.), then the line card CPU utilization becomes very high at the interrupt level. This greatly contributes to exhaustion of line card CPU resources and results in failure to process heartbeat keeaplives. As a result, line card is eventually reset by the SP to attempt recovery. Cause of the CPU being so frequently interrupted are the continuous interface state transitions which are triggered by the line card.

Passing CLIs to the line card fail:

```
7600#remote command module 2 sh proc cpu sort
No response from remote host
```

SP fails to receive heartbeat checks from the ES20 LC and eventually crashes

```
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 30 seconds
[2/0]
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 60 seconds
[2/0]
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 90 seconds
[2/0]
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 120 seconds
[2/0]
%CPU_MONITOR-SP-6-NOT_HEARD: CPU_MONITOR messages have not been heard for 150 seconds
[2/0]
%OIR-3-CRASH: The module in slot 2 has crashed
```

When unplugging the fibers, LC becomes responsive, but shows high CPU in interrupt:

```
7600#remote command module 2 sh proc cpu sort | e 0.00% 0.00% 0.00%
CPU utilization for five seconds: 99%/96%; one minute: 36%; five minutes: 23%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
124 59128 542 109092 2.19% 2.17% 2.30% 0 Vlan Statistics
134 221872 1057 209907 0.42% 8.74% 10.38% 0 CFIB LC STATS Ta
127 24072 3340 7207 0.18% 0.20% 0.17% 0 BW Stats Poll
213 1628 177 9197 0.12% 0.07% 0.05% 0 sip10g Stats Bac
173 7208 634 11369 0.12% 0.01% 0.00% 0 TCAM Manager pro
193 1240 177 7005 0.12% 0.05% 0.05% 0 MFI LFD Stats Pr
172 2488 373 6670 0.12% 0.08% 0.09% 0 QoS SP Process 104 440 87 5057 0.12% 0.04% 0.01%
0 xcvr RPC process
```

Conditions: Occurred on a Cisco 7600 router with a XFP-10GZR-OC192 housed in a ES20, where the optical fiber has its RX level out of the specified range for the given XFP being used. Problem exists in SPA driver code and can be seen on all line cards on which affected SPAs are supported.

Workaround: Verify the optical properties of the fiber using the **sh hw-module subslot X/Y transceiver Z stat** command. If out of range, replace with optical fibers for which the optical transmission properties are within the specified range for the given XFP being used.

- CSCsm66678

  Symptoms: Packets are not getting policed in MPLS cloud, causing the **show policy-map int** command to display incorrect counts. Conform and exceed actions are not being performed.

  Conditions: Even though packets are getting classified correctly, policing is not working on those packets.

  Workaround: There is no workaround.

  Further Problem Description: Policing is not working in the MPLS cloud. Consider the following three scenarios:

  1) When a service policy and MPLS are configured on the subinterface, policing works fine. 2) When a service policy and MPLS are configured on the main interface, policing works fine. 3) When a service policy is attached on the main interface and MPLS on the subinterface, policing does not work.

The first two cases work fine. It means if the MPLS feature and policy are on the main interface or the MPLS feature and policy are on the subinterface, policing works correctly. The problem is with the third case. Here, the MPLS feature is applied on the subinterface and policy on the main interface. If we do not have MPLS configured and we are receiving just IP packets, then all cases work fine. But MPLS packets are treated as IP packets.

- CSCsm74143

  Symptoms: INTR_MGR-DFC7-3-BURST: msg seen when PMAP is removed from subinterface.

  Conditions: Occurs on a ES20 LC with subinterface having a HQoS policy applied. The steps are:

  1) Remove the child policy from the parent class.

  2) Remove the service-policy from the subinterface.

  Workaround: Apply the service-policy again in the interface and remove the policy.

- CSCsm75286

  Symptoms: A route-map which is configured with both IPv4 and IPv6 for a BGP peer does not work as expected

  Conditions: Observed after the route-map is modified to delete a sequence.

  Workaround: Apply a fresh route-map

- CSCsm89795

  Symptoms: The router keeps reloading and complaining about unavailability of memory.

  Conditions: This symptom is observed if the router is directly connected to a DHCP server or if an attack is made by flooding DHCP replies.

  Workaround: There is no workaround.

- CSCso04932

  Symptoms: Traffic is lost for up to 30 seconds on a static route with next hop over ATM interface.

  Conditions: Occurs when next hop goes over an ATM interface.

  Workaround: There is no workaround.

- CSCso27236

  Symptoms: Cisco IOS CA shows incorrect renew date (Jan 1 1979). Example:

  Before restart Start Date:

  ```
  1 Jan 2008 10:00:00 End Date : 1 Jan 2011 10:00:00 Renew Date : 1 Jan 2008 09:58:00
  ```

  After restart Start Date:

  ```
  1 Jan 2008 10:00:00 End Date : 1 Jan 2011 10:00:00 Renew Date : 1 Jan 1970 08:00:00
  ```

  Conditions: Occurs when auto-enroll is enabled and the router is reloaded.

  Workaround: There is no workaround.

- CSCso39217

  Symptoms: Link flaps and causes traffic loss as well as repeated route convergence on RP.

  Conditions: Seen When ESM20 is reset. During stateful switchover (SSO), though not consistent. After a SSO switchover, we see a PORT_BOUNCED error message which indicates the cause of failure as the Consistency Check IDB was down.

  Workaround: There is no workaround.

- CSCso46337

  Symptoms: After stateful switchover (SSO), a traceback is seen.

Conditions: Occurs after SSO.

Workaround: There is no workaround.

- CSCso46427

  Symptoms: A device may crash when the **show clns interface** command is issued on the wrong interface.

  Conditions: The symptom is observed when there are a number (around 100 or more) CLNS interfaces on the device.

  Workaround: There is no workaround.

- CSCso48665

  Symptoms: With COPP configured, L2 traffic coming from VPLS SVI is punted to the RP and is subject to the control plane policy.

  Conditions: The symptom is observed on a Cisco 7600 series router with both VPLS SVI and COPP configured.

  Workaround: There is no workaround.

- CSCso50347

  Symptoms: A router may crash after the command **show ip bgp** *l2vpn vpls* **all prefix- list** is issued.

  Conditions: The symptom is observed when the **show ip bgp** *l2vpn vpls* **all prefix-list** command is used with a configured prefix-list.

  Workaround: Use the **show ip bgp** *l2vpn vpls* **all** command.

- CSCso56413

  Symptoms: A Catalyst 6000 line card may crash while attempting to free non-chunk memory.

  Conditions: Occurs when MAC out-of-band synchronization is enabled in a distributed forwarding system

  Workaround: There is no workaround

- CSCso57001

  Symptoms: Router crashes when interfaces flap and the device is running the MetroE IPSLA feature.

  Conditions: When the device is set to automatically start jitter/ping probes and the interfaces flap, it results in a crash when trying to re-create auto generated MetroE operations.

  Workaround: There is no workaround.

- CSCso59251

  Symptoms: An interface on ESM20G goes down.

  Conditions: Occurs when the interface has a 50 EVC on it. Seen on router using rsp72043-adventerprisek9_wan_dbg-mz.srb_throttle_033008 image.

  Workaround: A **shut/no shut** will correct the symptom.

- CSCso59974

  Symptoms: BGP session goes idle.

  Conditions: Occurs following a stateful switchover (SSO).

  Workaround: There is no workaround.

- CSCso62193

Symptoms: The standby router may reset unexpectedly.

Conditions: The symptom is observed when removing the frame relay map on the active using the **no frame-relay vc-bundle** command. The issue occurs because the frame relay map is removed in active but not in standby due to a synchronization problem.

Workaround: There is no workaround.

- CSCso88199

  Symptoms: When an MPLSoGRE tunnel is configured, and a packet is sent through the tunnel with the DF bit set in the outer IP header.

  Conditions: The tunnel encapsulation should be removed by the other end of the tunnel. But when DF bit is set in the IP header, this decapsulation did not happen.

  Workaround: There is no workaround.

- CSCso98143

  Symptoms: At boot up router may crash with the following error messages:

  ```
  %IPC-2-ONINT: Invalid operation at interrupt level: IPC blocking send request
  icc_send_request_internal: ipc_send_rpc_blocked failed, result 8
  ```

  Conditions: Occurs on Cisco 7600 configured with VRF-Lite aware PBR route-maps and running Cisco IOS Release 12.2SR or Cisco IOS Release 12.2SRC.

  Workaround: There is no workaround.

- CSCsq05680

  Symptoms: The Route-Processor may sometimes crash on reset of the ES20 linecard.

  Conditions: The symptom is observed when an ES20 card has ports as members of a port-channel.

  Workaround: There is no workaround.

- CSCsq15198

  Symptoms: When all uplink ports on SUP are admin down and a **no shut** is entered on any of the two uplink ports, BFD sessions running on a different LC on the chassis begin flapping.

  Conditions: This occurs whenever the first of two uplink ports is brought up.

  Workaround: There is no workaround.

- CSCsq18756

  Symptoms: MTR (with multi-session capability) is enabled by default and cannot be disabled. Old CE routers do not understand the multi-session capability therefore they disconnect the BGP session with notification.

  Conditions: The symptoms are observed when the MTR feature is enabled as default and when multi-session capability is sent in the default BGP peer.

  Workaround: There is no workaround.

- CSCsq18938

  Symptoms: WS-6708 is reset due to diag failure.

  Conditions: Occurs when traffic level is high. Traffic could be multicast bi-directional or L2 feature.

  Workaround: Disable health monitoring tests on the WS-6708

  Further Problem Description: When traffic is running, 6708 card gets reset due to TestFabricCh0Health HM test failures. The card will continuously reset with these messages:

  ```
  May 6 13:32:09.915 EDT: %PIM-5-NBRCHG: neighbor 10.252.3.130 DOWN on interface
  Port-channel10 non DR
  ```

```
May 6 13:32:09.307 EDT: %CONST_DIAG-SP-6-HM_TEST_SP_INFO: TestFabricCh0Health[3]:
last_busy_percent[8%], Tx_Rate[894], Rx_Rate[2454]
May 6 13:32:09.307 EDT: %CONST_DIAG-SP-2-HM_MOD_RESET: Resetting Module 3 for software
recovery, Reason: Failed TestFabricCh0Health
May 6 13:32:09.307 EDT: %OIR-SP-3-PWRCYCLE: Card in module 3, is being power-cycled
off (Diagnostic Failure)
```

- CSCsq24171

  Symptoms: Traffic may not flow on an encapsulation untagged EVC after an OIR.

  Conditions: The symptom is observed on an EVC on a physical port with encapsulation untagged, when the linecard is OIR. It is specific to EVC on the ES20 linecard.

  Workaround: Reapply the configuration on the specific interface.

- CSCsq30261

  Symptoms: eBGP sessions (with 200 VRF) on PE-CE keep flapping when sending traffic rate at 200 frames per second (FPS). At 50FPS they are stable.

  Conditions: Occurs when PE is connected to test device that is emulating 200 CE farms.

  Workaround: Perform a **shut/no shut** on the interface of the PE facing CE.

- CSCsq36191

  Symptoms: When an RP's CPU memory is almost all consumed (by BGP and/or other processes), repeated use of the **show ip bgp summary** command may cause a router to crash.

  Conditions: The symptom is observed when memory is almost all consumed and the command **show ip bgp summary command** is used repeatedly.

  Workaround: Upgrade to more memory.

- CSCsq44823

  Symptoms: The route target (RT) is not sent in BGP VPNv4 extended-community.

  Conditions: This symptom may be observed with Cisco IOS Release 12.2(33)SB when the router uses BGP VPNv4 update to send MDT information to the peer, which does not support IPv4 MDT SAFI.

  Workaround: There is no workaround.

- CSCsq45761

  Symptoms: Traceback may occur when TE tunnels are configured and after HA is done by script.

  Conditions: The symptom is observed on a Cisco 7600 series router and when TE tunnels and dot1q are configured on a CE-facing interface. This issue is only seen when HA uses a script.

  Workaround: There is no workaround.

- CSCsq50535

  Symptoms: Split-horizon may not work correctly for a Layer 2 Protocol Tunnelling (L2PT) packet received from a VPLS VC.

  Conditions: The symptom is observed on a Cisco 7600 PE router that is running VPLS and L2PT. The issue causes the L2PT packets to be sent back to the MPLS cloud on the other VPLS VC that is part of the same VFi, despite split- horizon being present. When there are multiple Cisco 7600 PE routers in the VPLS with similar configurations, there may be a loop of L2PT packets between the PEs.

  Workaround: Avoid using L2PT with VPLS.

  Alternate Workaround: Use Cisco IOS Release 12.2(33)SRA6.

- CSCsq52741

Symptoms: A VPN routing/forwarding (VRF) static route pointing to a next hop in global table is not installed in RIB after a reload of a Cisco 7600.

Conditions: The device is running Cisco IOS Release 12.2(33)SRB3 with single Supervisor. The interface in global table the next hop is reachable through, is a Ten Gigabit subinterface with **ip vrf receive** <*vrf name*> and policy routing enabled.

Workaround: Apply the VRF static route after the reload.

- CSCsq58385

  Symptoms: Cannot ping Hot Standby Routing Protocol (HSRP) virtual address when active on ES20 card.

  Conditions: This symptom is observed on a Cisco 7600 series router with SUP720, ES20 and running Cisco IOS Release 12.2(33)SRB3.

  Workaround: There is no workaround.

- CSCsq59977

  Symptoms: EOAM monitoring of CRC errors may not work with 6148A-RJ45 and 6148- FE-SFP linecards.

  Conditions: The symptom is observed when packets with errors are received. It is seen with 6148A-RJ45 and 6148-FE-SFP linecards.

  Workaround: There is no workaround.

- CSCsq63731

  Symptoms: If either the command **vlan-id dot1aq** *vlan-id* or the command **vlan-range dot1aq** *start-vlan-id end-vlan-id* is configured on a main interface which is also configured for routing, and an ARP packet is sent to the router on the configured VLAN, then the router may send an ARP reply with a VLAN ID of zero.

  Conditions: The symptoms are seen on a router when the command **vlan-dot1q** *vlan-id* is configured on a GigabitEthernet interface and **encapsulation dot1q** *vlan- id* is configured on a FastEthernet interface.

  Workaround: Change the router's (CE) configuration to use a sub-interface for the vlan-id instead of using the **vlan- dot1q** *vlan-id* command on the main interface. With a sub-interface configured on the router, we can verify that the ARP packets are sent with proper VLAN ID.

- CSCsq77043

  Symptoms: A Cisco IOS device configured for an Embedded Event Manager (EEM) Tool Command Language (TCL) policy that uses the TCL CLI library may have the policy hang if the devices hostname is longer than 20 characters long.

  Conditions: If the device is configured with a TCL policy that uses the **cli_open** TCL command and that device has a hostname longer than 20 characters the policy may hang.

  Workaround: Reduce the size of the hostname.

- CSCsq78100

  Symptoms: On a LAN card if **wrr-queue cos-map** is changed on a port that is never up, some packets are dropped on another port.

  Conditions: Occurs under the following scenario:

  1.) WRED is disabled in the port that is sending traffic.

  2.) Configure **wrr cos-map** on another port that is never up.

  Workaround: Configure **wrr cos-map** only after the port is **no shut**.

- CSCsq79253

  Symptoms: Once a packet buffer error is detected on a Pinnacle, traffic loss may occur after recovery.

  Conditions: The symptom is observed after the first packet buffer error is detected. During the first error detection, some interrupts are not re- enabled, leading to problems detecting and correcting subsequent errors.

  Workaround: Reload the affected module.

- CSCsq81235

  Symptoms: A VRF cannot be configured again when it is deleted by using the **no ip vrf** command.

  Conditions: This symptom is seen only on VRFs with an MDT tunnel.

  Workaround: There is no workaround.

- CSCsq86014

  Symptoms: When removing a subinterface on a Cisco 7600 series router, connectivity issues might occur on other subinterfaces that are part of the logical main interface.

  Conditions: The symptom is observed on an ES20 linecard and with Cisco IOS Release 12.2(33)SRB3 and Release 12.2(33)SRC1. It is seen when the configuration requires double-tagging. With a back-to-back connection, a QinQ sub-interface is created on either side and an IP address is assigned. Then, another sub-interface with the same outer VLAN is created and then removed.

  Workaround: Use the **shutdown no shutdown** command sequence to restore connectivity.

- CSCsq91960

  Symptoms: VRF may not get deleted if the VRF NAME size is 32 characters on a dual RP HA/SSO router.

  Conditions: This symptom occurs when adding a VRF with 32 characters on a DUAL RP HA router. (In some releases a VRF name with more than 32 characters will get truncated to 32.) The following may occur:

  - There may be a DATA CORRUPTION ERRMSG. - While deleting this 32 character length VRF, VRF will fail to get deleted completely with an ERRMSG on active.

  Workaround: There is no workaround.

- CSCsq98626

  Symptoms: On a Cisco 7600 configured for ATM Circuit Emulation (CEM) over MPLS, there are errors reported under the CEM circuit. This is observed using the **show cem circuit** command.

  Conditions: The error is only observed when the core-facing interface has these characteristics:

  - SVI i.e L2 (Bridge-domain and Switchport) - The physical interface is from a ES20 module

  Workaround: Disable MAC address aging with the **mac-address-table aging-time 0** command.

- CSCsr08921

  Symptoms: Cisco 7600 RP crashes when pseudo-wire is down for ATM over MPLS over GRE and when AAL0 encapsulation is used. The problem happens in customer-facing SIP-400 line card.

  Conditions: Configure ATM AAL0 over MPLS over GRE, then bring the pseudo-wire down.

  Workaround: There is no workaround.

- CSCsr09173

Symptoms: After an Not-So-Stubby Area (NSSA) ABR reload, the default LSA may fail to generate on some NSSAs.

Conditions: The symptom is observed following a reload or other circumstances like interface flapping.

Workaround: Reconfigure the area as NSSA by the following command sequence: **no area** *number* **nssa no- summary** followed by **area** *number* **nssa no-summary**.

- CSCsr11085

  Symptoms: A single route loop whose gateway is covered by a default route remains in the RIB after a more specific route which resolves the gateway is removed. For example, the following routes may exist in the RIB:

  ```
  S* 0.0.0.0/0 is directly connected, Ethernet1/0
  S 192.168.0.0/16 [1/0] via 192.168.1.2
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
  C 192.168.1.0/24 is directly connected, Ethernet0/0
  L 192.168.1.1/32 is directly connected, Ethernet0/0
  192.169.1.0/24 is variably subnetted, 2 subnets, 2 masks
  C 192.169.1.0/24 is directly connected, Ethernet1/0
  L 192.169.1.1/32 is directly connected, Ethernet1/0
  ```
  If interface eth 0/0 goes down, then we have the following:

  ```
  S* 0.0.0.0/0 is directly connected, Ethernet1/0
  S 192.168.0.0/16 [1/0] via 192.168.1.2
  192.169.1.0/24 is variably subnetted, 2 subnets, 2 masks
  C 192.169.1.0/24 is directly connected, Ethernet1/0
  L 192.169.1.1/32 is directly connected, Ethernet1/0
  ```
  and

  ```
  Router#show ip route loop
  ->default:ipv4:base 192.168.0.0/16 -> base 192.168.1.2 static 00:01:07 N
  ```
  In this case the route:

  ```
  S 192.168.0.0/16 [1/0] via 192.168.1.2
  ```
  should be removed from the RIB.

  Conditions: The default route must be present in order for the above behavior to be considered wrong. If a default route is NOT present then the route

  ```
  S 192.168.0.0/16 [1/0] via 192.168.1.2
  ```
  is a misconfiguration and must be corrected by altering the configuration. Until the configuration is corrected, the route will remain in the RIB and traffic covered by that route will be dropped.

  Workaround: The one route loop can be removed from the RIB using the **clear ip route** command:

  ```
  clear ip route 192.168.0.0
  ```
  Further Problem Description: In the absence of the default route removal of the one route loop can lead to oscillation, which would seriously degrade the performance of the router.

- CSCsr26025

  Symptoms: When "0.0.0.0/8 static route to null 0" is configured, the default gateway failover does not work. RIB is not updated.

  Conditions: Occurs under the following scenario:

  - Border Gateway Protocol (BGP) with two neighbors sending a default gateway.

  - Static route “0.0.0.0/8 to null 0” is configured.

  - Failover takes place and RIB is not updated.

  Workaround: There is no workaround.

- CSCsr40433

Symptoms: Traffic engineering (TE) tunnel reoptimization fails and tunnel stuck in “RSVP signaling proceeding”.

Conditions: Occurs when explicit path with loose next hops and one of the next hops is still reachable and that next hops is a dead-end.

Workaround: Use strict next hop addresses.

- CSCsr49316

  Symptoms: A crash happens when the **show ipv6 rpf x:x:x::x** command is given.

  Conditions: This symptom is observed only when there are more than 16 adjacencies for a single static route. The crash happens when the **show ipv6 rpf** command is given for this particular static route.

  Workaround: There is no workaround. This problem occurs as long as there are more than 16 adjacencies for single static route even if some of them are not active.

- CSCsr55278

  Symptoms: Fast switching of multicast packets may not occur on the interface of a PE router. All multicast packets are forwarded in process switching.

  Conditions: The symptom is observed after the interface is changed from a forwarding interface of one VRF to another VRF.

  Workaround: There is no workaround.

- CSCsr55990

  Symptoms: HSRP virtual MAC is dynamic instead of static on a Cisco 7600 after a reload.

  Conditions: HSRP is configured under a routed vlan-based pseudowire:

  interface Vlan X ip address 10.0.0.1 255.255.255.0 standby 1 ip 10.0.0.254 xconnect x.y.z.w encapsulation mpls

  Occurs when fast millisecond HSRP timers are used, and an HSRP interface delay is not configured.

  Workaround: Perform a **shut/no shut** on the interface "vlan X". Or, as a preventive action, configure **standby delay minimum 60** on the interfaces. Testing has shown that after a reboot the entry is installed correctly in the PFC/DFC.

- CSCsr58334

  Symptoms: Ping packets are blocked.

  Conditions: Occurs after configuring split-horizon.

  Workaround: There is no workaround.

- CSCsr59284

  Symptoms: Memory allocation fails. Sometimes neighbor relationship also drops.

  Conditions: Happens after entering **show mem** command. After the system booted up, while the Cisco 7600 system was receiving the BGP routes, the command is entered. Upon hitting the space key to scroll the windows for two to three times. The following errors are displayed:

  ```
  "%COMMON_FIB-3-NOMEM: Memory allocation failure for CEF: terminal fibs list in IPv4
  CEF [0x08812F1C] (fatal) "
  ```

  Workaround: Enter the **show mem sum** command.

- CSCsr72959

  Symptoms: Router crashes.

  Conditions: Occurs after entering **no service dhcp**.

Workaround: There is no workaround.

- CSCsr74002

  Symptoms: In some scenarios, UDLD packets received on a dot1q tunnel port in a VLAN where a Virtual Private LAN Services (VPLS) VFI is attached may be flooded to the VPLS VLAN without being processed locally. This may lead to port being err-disabled.

  Conditions: Occurs when some port configured as dot1qtunnel port in the VPLS VLAN. It will not process the received UDLD packet on those tunnel ports and will instead send them to the VPLS. If the VLAN interface with the VFI is shutdown, UDLD is processed normally.

  Workaround: Disable UDLD or enable spanning-tree in vfi vlan.

- CSCsr82785

  Symptoms: If APS is configured on a large number of channelized sub-interfaces associated with a single controller such that a single failure can cause all of these interfaces to failover at the same time, and RIP is configured to run over these interfaces, high sustained CPU usage will be seen following the failover and reconvergence time will be lengthy.

  Conditions: Large number of APS protected interfaces fail over at the same time. RIP is the protocol running on those interfaces. IP addresses on all interfaces are covered by the same network statement.

  Workaround: There is no workaround.

  Further Problem Description: The length of the high CPU and reconvergence period will increase as the number of impacted interfaces increases.

  The length of the high CPU and reconvergence period will also increase as the number of network statements which cover the IP addresses on the affected interfaces decreases i.e. it will be worst when a single classful network (e.g. 10.0.0.0) covers all interfaces, somewhat better when multiple classful networks are impacted.

- CSCsr86515

  Symptoms: Router crashed due to watchdog timeout in the virtual exec process.

  Conditions: This was observed on a Cisco 7600 running Cisco IOS Release 12.2(33)SRB3 after a ATM sub-interface was removed.

  Workaround: There is no workaround.

- CSCsr96042

  Symptoms: Router crashes.

  Conditions: Occurs if “ip vrf” is deleted from the configuration.

  Workaround: Remove “ip vrf forwarding” from all interfaces in the VRF before removing the VRF.

- CSCsr99533

  Symptoms: Lawful Intercept (LI) may not work when accelerated LI feature is used and LI replication is being done by the supervisor card.

  Conditions: Occurs on a Cisco 7600 configured with a RSP720 supervisor card.

  Workaround: Use SIP400 as accelerated LI module.

- CSCsr99630

  Symptoms: Packets drop in the tail of MPLSoGRE tunnel.

  Conditions: Occurs when an MPLSoGRE tunnel is configured, and a packet is sent through the tunnel with the DF bit set in the outer IP header.

Workaround: There is no workaround.

- CSCsr99933

  Symptoms: Routers running Cisco IOS Release 12.2(33)SRB4 experiencing high CPU usage.

  Conditions: Occurs with high purge rate of 180/sec and above.

  Workaround: There is no workaround.

- CSCsu05525

  Symptoms: After removing the “default-originate” configuration, the default-route is not withdrawn.

  Conditions: Occurred on a router running Cisco IOS Release 12.2SR.

  Workaround: Clear the session to remove the configuration.

- CSCsu24087

  Symptoms: A router hangs for a couple of minutes, then crashes anytime the **clear ip bgp neighbor x.x.x in** command is issued.

  Conditions: This symptom occurs when a router crashes when the **clear ip bgp neighbor x.x.x.x soft in** command is issued when the following commands are configured for that neighbor (without route-map): 1) **neighbor x.x.x.x soft-reconfiguration inbound** 2) **neighbor x.x.x.x weight** 3) **neighbor x.x.x.x filter-list in**

  If any one of the commands is not configured, then the router will not crash.

  Workaround: Configure route-map instead of filter-list for inbound direction. For example: “neighbor x.x.x.x filter-list 1 in” replace with “neighbor x.x.x.x route-map *name* in”

  where, route-map *name* permit 10 match as-path 1

- CSCsu57331

  Symptoms: In a Virtual Private LAN Services (VPLS) scenario with ESM20 as core facing interface, imposition traffic might fail.

  Conditions: Occurs only when ports from Bay 1 are used as core facing interface.

  Workaround: Reset the line card.

- CSCsu57958

  Symptoms: In a scenario where a Catalyst 6500 or Cisco 7600 performs DHCP snooping + DAI functionality and a second device acts as DHCP relay, it was observed that DHCP snooping database was not populated. DHCP snooping is configured in this case on the ingress VLAN (traffic from the DHCP clients) and the DHCP server can be reached on a different egress VLAN (DHCP requests are routed).

  DHCP Replies from the server (DHCPOFFER and DHCPACK) are not snooped by the Catalyst 6500 or Cisco 7600 and so bindings are not established. Consequence is that clients will get their own IP Address but ARP Inspection will fail because bindings were not learned on the device.

  Conditions: Occurs with DHCP Snoooping + DAI configured on a Catalyst 6500 or Cisco 7600 in a routed scenario (Ingress VLAN and Egress VLAN are different) and DHCP Relay performed by a different device.

  Workaround: Configure DHCP Snooping on both client and server side VLANs. Problem is applicable to both Cisco IOS Release 12.2(18)SXF and Cisco IOS Release 12.2(33)SRB.

- CSCsu62667

  Symptoms: LSP ID change after stateful switchover (SSO) due to failure in signaling recovered label switched path (LSP).

Conditions: Occurs following a SSO switchover.

Workaround: There is no workaround.

- CSCsu63884

  Symptoms: When platform sampling is configured (MLS sampling), PFC/DFC flows are sampled, while RP flows are not.

  Conditions: This leads to Netflow collectors that cannot be programmed for sampling configuration by engine ID to overestimate the RP-captured flows packet/byte counts.

  Workaround: There is no workaround.

- CSCsu88256

  Symptoms: Imposition traffic on a Ethernet Over MPLS (EoMPLS) VC is dropped.

  Conditions: Occurs if xconnect is configured on a EVC with switchport on another interface.

  Workaround: There is no workaround.

  Further Problem Description: When this problem happens the DMAC used by the imposition line card is that of the switchport interface instead of the router MAC address, causing the packet to be dropped.

- CSCsu89550

  Symptoms: All tagged packets on a hardware Ethernet Over MPLS (EoMPLS) VC is subjected to CoPP when the VC is down.

  Conditions: Occurs if VC is brought down by flapping core facing interface.

  Workaround: Remove the control-plane policy.

  Further Problem Description: It is applicable to only port-mode hardware EoMPLS.

- CSCsv04507

  Symptoms: Connectivity works initially, but with adding one queueing service policy and then removing it from the interface, breaks the connectivity between the end points.

  Conditions: Occurs on a DLFI link on ATM.

  Workaround: Perform a **shut/no shut** on the interface.

Resolved Caveats—Cisco IOS Release 12.2(33)SRB4

Cisco IOS Release 12.2(33)SRB4 is a rebuild release for Cisco IOS Release 12.2(33)SRB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRB4 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCea90968

  Symptoms: When you enter the **atm pvp vpi** interface configuration command on a Cisco 7206VXR, the router may reload unexpectedly and display the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address addr=0x40, pc=0x60202778,
  ra=0x60202780, sp=0x63BF1718
  ```

  Conditions: This symptom is observed on a Cisco 7206VXR that runs the c7200-js-mz image of Cisco IOS Release 12.3, 12.3 B, or 12.3 T and that is configured with a Network Processing Engine 225 (NPE-225).

Workaround: There is no workaround.

- CSCec51750

  Symptoms: A router that is configured for HTTP and voice-based services may reload unexpectedly because of an internal memory corruption.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3 or Release 12.3 T.

  Workaround: There is no workaround. Note that the fix for this symptom prevents the router from reloading and enables the router to generate the appropriate debug messages. The internal memory corruption is addressed and documented in caveat CSCec20085.

- CSCec80902

  Symptoms: A Cisco 7500 series that is configured for Hierarchical Queuing Framework (HQF) may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed when you attempt to print queue statistics for priority classes within the same layer of a policy map.

  Workaround: There is no workaround.

- CSCek74474

  Symptoms: When you enter the **protocol ip** *protocol-address* **broadcast** command on an ISP termination point, the command may not be applied to a connected CPE, preventing the CPE from populating its ARP cache and from properly forwarding traffic.

  Conditions: This symptom is observed on a Cisco router that functions as an ISP termination point and that is configured for point-to-point ATM connections when a connected CPE is configured for multipoint-to-point ATM connections.

  Reason: Command is not applied until VC recreated or bounced.

  Workaround: Configure the **protocol ip** *protocol-address* **broadcast** command as part of a PVC configuration on the CPE.

  Alternate Workaround: Configure the connection between the ISP termination point and the CPE as a multipoint-to-point ATM connection.

- CSCek75931

  Symptoms: A Cisco 10000 series router may experience a CPUHOG condition.

  Conditions: This condition is observed when there is an increase of more than 2000 sessions established.

  Workaround: There is no workaround.

- CSCsb63652

  Symptoms: BGP convergence is very slow, and CPU utilization at the BGP Router process is always near 100 percent during the convergence at the aggregation router. This issue obviously shows the following tendencies:

  1) The greater the number of component prefixes that belong to the aggregate- address entry, significantly slower convergence is seen at the aggregation router.

  2) The greater the number of duplicate aggregation component prefixes for the aggregate-address entry, seriously slower convergence is seen at the aggregation router.

  Conditions: Any release would be affected if "aggregate-address" is configured and routing updates are received every few seconds.

  Workaround: Remove the "aggregate-address".

Further Problem Description: If you configure "aggregate-address" lines after BGP convergence has been achieved, the BGP process only holds about 60 or 80 percent of the CPU for about 1 minute. However, if you do peer reset after "aggregate-address" entries have been configured, the convergence time is about 32 minutes (it is about 6 minutes if "aggregate-address" entries are removed).

- CSCsc87117

  Symptoms: Bidirectional designated forwarder flaps, and packets are looped in the network for up to 20 seconds.

  Conditions: Occurs when two bidirecitonal-enabled routers are servicing the last-hop receivers on 10 or more VLANs. There should be receivers on all 10 VLANs for a minimum of 1,000 groups. When the Reverse Path Forwarding (RPF) link of active designated forwarder (DF) is shut or when the link is brought back up, DF on the receiver VLAN needs to change from one box to another box. During DF-transition, the DF-election flaps and multicast packets are looped up to 20 seconds.

  Workaround: Configure the **mls ip multicast Stub** command on the receiver VLANs on both boxes.

- CSCsc94969

  Symptoms: After configuring **import ipv4 unicast map #name** under **ip vrf #name**, all existing routes (except direct connected) under the VPN routing/forwarding (VRF) table disappear.

  Conditions: Occurs when router is configured with MPLS, VRF, and import IPv4.

  Workaround: There is no workaround.

- CSCsd80349

  Symptoms: In a MPLS Traffic Engineering Fast Reroute environment, if the line protocol on the protected link goes down due to mismatched keep-alives on the link (or too many collisions), the forwarding plane does not switch traffic for protected label switched paths (LSP) to their respective backups.

  Conditions: Occur under the following scenario:

  – A Cisco router running a Cisco IOS Release 12.2S
  – Router acting as a Point of Local Repair (PLR) for MPLS Traffic Engineering Tunnels that request Fast Reroute protection
  – Mismatched keep-alives or excessive collisions on the protected link.

  Workaround: There is no workaround.

- CSCse55425

  Symptoms: When configuring a serial interface or issuing **show** commands related to that serial interface, a router may incorrectly configure a different serial interface or may show output from a different serial interface in the router.

  Conditions: The conditions under which the problem manifest itself are unknown, and appear to be random. The symptom exists only when using a channelized T3 card and configuring one of the T1's.

  Workaround: A router reload clears the issue.

- CSCsg21394

  Symptoms: A router reloads unexpectedly because of malformed DNS response packets.

  Conditions: This symptom is observed when you configure name-server and domain lookup.

  Workaround: Configure the **no ip domain lookup** command to stop the router from using DNS to resolve hostnames.

- CSCsg42672

  Symptoms: On a Cisco router running Cisco IOS Release 12.0(32)S4 and configured with BGP and peer-groups, if the Fast Peering Session Deactivation feature is configured in the peer-group, the router automatically configures on the command a route-map with the same name as the peer- group.

  Conditions: Occurs with the following configuration sequence:

```
RR#conf t
Enter configuration commands, one per line. End with CNTL/Z.
RR(config)#router bgp 65001
RR(config-router)#neighbor rrs-client fall-over ?
bfd Use BFD to detect failure
route-map Route map for peer route
<cr>
RR(config-router)#neighbor rrs-client fall-over
RR#sh ru
<snip>
router bgp 65001
neighbor rrs-client peer-group
neighbor rrs-client remote-as 20959
neighbor rrs-client update-source Loopback0
neighbor rrs-client fall-over route-map rrs-client <<<<<<<
the route-map does not exist.
```

  Workaround: Configure the neighbor individually or use peer-templates.

- CSCsh32655

  Symptoms: A router may crash when you remove a configuration that consists of multiple instances of BGP and the **ip access-list** command.

  Conditions: This symptom is observed on a Cisco router when you remove the configuration through a TFTP server.

  Workaround: Do not use a TFTP server to remove a BGP configuration.

- CSCsh73139

  Symptoms: IPv6 routes that are redistributed via the **redistribute connected** address family configuration command may disappear after you have performed an OIR of an Enhanced FlexWAN line card.

  Conditions: This symptom is observed on a Cisco 7600 series. Note that only IPv6 is affected, IPv4 works fine.

  Workaround: Disable and then re-enable the **redistribute connected** address family configuration command.

- CSCsh74025

  Symptoms: ATM packets are dropped, CLNS ping fails and Intermediate System-to-Intermediate System (IS-IS) adjacencies do not come up.

  Conditions: Occurs when **set atm-clp** is configured in service policy.

  Workaround: Remove the **set atm-clp** command from the service policy on the output interface.

- CSCsi51014

  Symptoms: Disk access causes router to crash.

  Conditions: Occurs after **fsck** execution.

  Workaround: Format disk, which causes the data loss on the affected disk.

- CSCsi92079

Symptoms: If an access control list (ACL) is used for a destination only prefix, a fatal error is declared and shuts down optimized edge routing (OER). For destination only traffic classes, prefix-list should be used, not ACL or access control entry (ACE).

Conditions: This behaviour is observed on Cisco IOS Release 12.4(11)T and later releases at this time.

Workaround: Use prefix list instead of ACL/ACE for destination only traffic classes. For example:

- use prefix list for a traffic class 10.1.1.0/24
- use ACE for traffic class 10.1.1.0/24 DSCP af11

- CSCsi97434

  Symptoms: The router will crash when IPSec is established only in the case when both PKI and IKE AAA accounting are configured.

  Conditions: This symptom occurs when PKI is configured, and the DN is used as the ISAKMP identity. The crash only occurs when the DN is not available, and the server tries to use the DN in the AAA accounting recording.

  Workaround: Do not use this configuration combination (PKI, DN as ISAKMP identity and AAA accounting).

- CSCsj19308

  Symptom: MLPPP/MLFR ping failure on SPA-2/4CT3 or SPA-CH-STM

  Conditions: MLPPP/MLFR configured on SPA-2/4CT3 or SPA-CH-STM

  Workaround: Reload the SPA using **hw-module** *subslot* <*slot*>/<*subslot*> **reload**

- CSCsj21785

  Symptoms: A Traffic Engineering (TE) tunnel does not re-optimize to explicit path after an MTU change.

  Conditions: The TE tunnel is operating via explicit path. The MTU on outgoing interface is changed. OSPF is flapped, and it does not come up as there is MTU mismatch (MTU is not changed on peer router). Meanwhile the TE re- optimizes to a dynamic path-option as expected. Now the MTU is reverted back to the previous value, and the OSPF adjacency comes up. The TE tunnel does not re-optimize to explicit path. Manual re-optimization of the TE tunnel fails as well, and the TE tunnel sticks to the dynamic path.

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

- CSCsj37111

  Symptoms: IPv4 inconsistencies and %FIB-4-FIBXDRINV error message upon reset of line card

  Condition: Problem observed on Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCsj50412

  Symptoms: There are two symptoms:

  1. Label Distribution Protocol (LDP) is not installing the outgoing label in Label Forwarding Information Base (LFIB) for a directly-connected static route with null next-hop.

  2. MPLS LFIB may not be updated following a quick LDP session flap. This may result in a "No Label" for outgoing label for the affected prefix.

  Conditions: Issue seen only when LDP flaps in a short interval.

Workaround: There is no workaround to prevent the issue. To recover enter the **clear ip route** *affected_prefix* command will trigger an install of the outgoing label.

Further Problem Description: LDP should have the label from the next-hop neighbor, but it does not update the LFIB. To confirm this, **show mpls ldp binding** <*prefix*> <*mask*> **detail** should show a label received from the appropriate neighbor.

- CSCsj58223

  Symptoms: Crash due to a bus error after the **show memory** command is entered.

  Conditions: Occurs on a WS-C6509-E running Cisco IOS Release 12.2(18)SXF8. It happens very rarely.

  Workaround: Do not use the **show memory** command.

- CSCsj89712

  Symptoms: Using **scp** to copy files from disk to SSH server is extremely slow. It takes more than 2 minutes to get the prompt back after launching the command to copy a small file.

  Conditions: This has been seen on a Cisco 7600 router running Cisco IOS Release 12.2(33)SRA4 or Cisco IOS Release 12.2(33)SRB.

  Workaround: Use another form of copy.

- CSCsk03336

  Symptom: Interface counters on line cards may show incorrect packet input statistics in the output of the **show interface** command.

  Conditions: Occurs when the "CEF LC IPC Backg" process causes the line card CPU to exceed 90%. This is seen when an unstable network causes excessive CEF updates.

  Workaround: There is no workaround.

- CSCsk13725

  Symptoms: When using SNMP to poll IP SLA (SAA/RTR) information on a router, the device gets stuck on one value. This can cause the network management application to timeout or sometimes crash

  Conditions: This problem is only happening when polling the CISCO-RTTMON-MIB via snmp get.

  Workaround: Instead of SNMP, use the command-line interface to retrieve the information.

- CSCsk21328

  Symptoms: Router crashes during shutdown or deletion of interface.

  Conditions: Occurs on interfaces on which IPv6 is enabled.

  Workaround: There is no workaround.

- CSCsk26973

  Symptoms: A router that is running NHRP leaks memory when many incomplete cache entries are created. The incomplete cache entries can be verified by typing the **show ip nhrp** command and looking for "type incomplete". The memory leaked can be seen by examining the output of the **show chunk** command and looking for "NHRP Cache".

  Conditions: This symptom could occur when traffic to nonexistent or non- responding addresses are forwarded by the router over the DMVPN/NHRP cloud.

  Workaround: There is no workaround.

- CSCsk35241

Symptoms: BGP sessions on a scaled setup, like 800 eBGP peers, can sometimes get into a situation where BGP sessions go into active state only to be cleaned up later and then start anew. The router could be perpetually in this race condition once this occurs, not allowing the router to establish BGP sessions.

Conditions: The problem was seen on a line card online insertion and removal (OIR) on a Cisco 7600 router.

Workaround: Use the **clear ip bgp *** to correct the problem.

- CSCsk35985

  Symptoms: The system crashes when the **show ipv6 ospf lsdb- radix** hidden command is entered.

  Workaround: Do not enter the **show ipv6 ospf lsdb-radix** command.

- CSCsk36324

  Symptoms: On a Cisco router, OSPF might go into a loop during SPF calculation, causing high CPU utilization and rendering the router inaccessible.

  Conditions: This symptom occurs when router LSAs with a link metric disallowed by RFC 2328 are present in the network (note that Cisco routers do not originate such LSAs) and when the network is unstable (link flapping during the SPF calculation).

  Workaround: To fix the problem, reload the router. To prevent the problem, manually configure a link metric according to RFC 2328.

  Important Note: CSCsk36324 caused MPLS TE defect CSCsl18176 and has been backed out under defect CSCsl18176. A new fix for this issue will be committed under defect CSCsl32318.

- CSCsk66339

  Symptoms: A Cisco 7600 router running Cisco IOS Release 12.2(18)SFX6 may encounter a condition such that when intermediate system-to-intermediate system (IS-IS) and traffic engineering (TE) are configured, IS-IS should remove the native path from its local RIB and call RIB code to remove the path from global RIB but fails by either not passing the "delete" msg to RIB properly or RIB does not react when it received the "delete" call.

  Conditions: The **show mpls traffic-engineering tunnel** command output may indicate "Removal Trigger: setup timed out" status.

  Workaround: Perform a **shut/no shut** on the interface or change the metric temporarily to force an update with the **tunnel mpls traffic-eng autoroute metric 1** command.

- CSCsk69186

  Symptoms: Walking entSensorThresholdTable of CISCO-ENTITY-SENSOR-MIB, with ES20 module in the chassis causes router to crash.

  Conditions: Occurs when ES20 module is present during mibwalk.

  Workaround: Create a view and exclude CISCO-ENTITY-SENSOR-MIB from that view.

- CSCsk93241

  Cisco IOS Software Multiprotocol Label Switching (MPLS) Forwarding Infrastructure (MFI) is vulnerable to a Denial of Service (DoS) attack from specially crafted packets. Only the MFI is affected by this vulnerability. Older Label Forwarding Information Base (LFIB) implementation, which is replaced by MFI, is not affected.

  Cisco has released free software updates that address this vulnerability.

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

- CSCsl16323

Symptoms: Traceback with the following message displayed:

```
PST: %COMMON_FIB-4-FIBNULLIDB: Missing idb for fibidb VRF_0_vlan1020 (if_number 132).
```

Conditions: This traceback is seen after doing stateful switchover.

Workaround: There is no workaround.

- CSCsl19708

  Symptoms: Fabric Channel may not go into sync on bootup.

  Conditions: Can occur in any enviornment, but error is only seen during bootup.

  Workaround: There is no workaround.

- CSCsl46846

  Symptoms: Channel-group command disappears from the interface after reboot when channel-group is configured with outbound service policy.

  Conditions: Happens only with QoS configuration.

  Workaround: Reconfigure channel-group after bootup.

- CSCsl52220

  Symptoms: The **snmp ifindex persist** command is incorrectly enabled on some interfaces.

  Conditions: This issue affects interfaces with similar interface descriptors. For example, if the command is enabled on Ethernet 0/1, it will be enabled on Ethernet 0/10 to Ethernet 0/19.

  Workaround: There is no workaround.

- CSCsl61164

  Symptoms: Router may crash @ipflow_fill_data_in_flowset when changing flow version.

  Conditions: Occurs when netflow is running with data export occurring while manually changing the flow-export version configuration from version 9 to version 5 and back to version 9 again.

  Workaround: Do not change the netflow flow version while the router is exporting data and routing traffic.

- CSCsl65327

  Symptoms: Unable to write a large file when the file size is larger than the NVRAM size, even when **service compress-config** is enabled.

  Conditions: Occurs when a large configuration file is copied to startup-config when the file is larger than the NVRAM size

  Workaround: Copy the file to running-config and then issue the **wr mem** command.

- CSCsl70729

  Symptoms: Following switchover, state sync to standby for 2,000 layer 2 virtual circuits takes 4-5 minutes, during which CPU usage is also very high (99%).

  Conditions: This was observed with 2,000 anything over MPLS (AToM) circuits configured for nonstop forwarding (NSF) and stateful switchover (SSO).

  Workaround: There is no workaround.

- CSCsm01126

  Symptoms: The standby fails to come up in SSO. The following message is seen on the active:

  ```
  %FILESYS-4-RCSF: Active running config access failure (0) <file size>
  ```

  Conditions: This symptom is observed when the router has a configuration greater than 0.5 megabytes.

Workaround: There is no workaround.

- CSCsm15687

  Symptoms: Configuration of the **crypto connect vlan <x>** command may fail when the command is applied to a dot1q subinterface.

  Conditions: Occurs on a system with 7600-SIP-600 linecards and GE SPAs installed.

  Workaround: There is no workaround.

- CSCsm17983

  Symptoms: Router experiences memory corruption.

  Conditions: Unknown conditions. Appears to be random.

  Workaround: There is no workaround.

- CSCsm21435

  Symptoms: Clock accuracy goes out of conformance when the reference clock is reverting from the secondary source to the primary after a switchover.

  Conditions: Occurs when dual Circuit Emulation over Packet (CEoP) cards are receiving reference clock via each one's BITS-IN.

  Workaround: There is no workaround.

- CSCsm26130

  Symptoms: When removing a subinterface from the configuration that contains an IP address that falls into the major net of the static route, the static route is no longer injected into the BGP table. Since the route is not in the BGP table, it is not advertised to any peers.

  Conditions: This symptom is observed with auto-summary enabled in BGP. A static summary route is configured to null0 and is injected into the BGP table with a network statement.

  Workaround: There are four possible workarounds:

  1) Use an "aggregate-address" configuration instead of the static route to generate the summary.

  2) Remove auto-summary from the BGP process.

  3) Enter the **clear ip bgp *** command.

  4) Remove and reconfigure the BGP network statement for the summary route.

- CSCsm44147

  Symptoms: The standby WS-SUP720-3BXL failed to boot into SSO mode because of MCL check failure with the FPD configuration command: **upgrade fpd path sup-bootdisk:**

  Conditions: The problem happens when "sup-bootdisk:" is used as the FPD image package directory path argument in the **upgrade fpd path** *pkg-dir-path* configuration command for an active WS-SUP720-3BXL that supports "sup-bootdisk:" filesytem, but the same fiilesystem is not support by the standby WS-SUP720-3BXL.

  Workaround: For systems that have a mixture of old and new WS-SUP720-3BXL, please do not use "sup-bootdisk:" as the filesystem in the **upgrade fpd path** *pkg-dir-path* configuration command, instead use the "sup-bootflash:" filesystem as this filesystem exist on both old and new WS-SUP720-3BXL.

  Further Problem Description: The **show module** EXEC command can be used to identify the HW revision of the WS-SUP720-3BXL, if it does not have a version above 5.x then it won't have the support of the "sup-bootdisk:" filesystem.

- CSCsm44620

Symptoms: Multicast tunnel not coming up after RPM change. A misconfiguration with overlapping networks causes the join to be rejected. This can be seen on the PIM neighbor list.

Conditions: There is a problem related to one of the hub card in rpm-xf.10 in forwarding PIM traffic from 2 PEs (rpm-xf.13 & rpm-xf.11). After RP migration from AVICI to CRS we found that tunnels from PE in slot 13 were not coming up. PE in slot 13 was in consistently in registering mode. PE was not coming out of registering mode which was preventing the tunnels from coming up. For PE to come out of registering mode S,G state should be built from new RP down to PE. At this stage the CRS (RP) showed that S,G tree was establish at the RP. S,G tree was OK all the way down from CRS to the last hop (P in slot 10) connecting to the slot 13 PE. The P router in slot 10, which is directly connected to PE, showed that S,G state was established and PE facing interface was in OIL. But there were couple of discrepancies on the P in slot 10. There were no flags set on this P for the mroute of PE. In addition, we found that PE was not receiving any PIM traffic from the P in slot 10. This led to suspicion that although the P showed the correct S,G and OIL but is still not able to forward traffic to the PE. And this could be the reason for PE to remain in registering mode hence preventing the tunnels from coming up.

Workaround: Remove the following configurations:

a. rpm-xfh10-z135 - shut & remove interface Switch1.4073

b. rpm-xfh09-z134 - shut & remove interface Switch1.4073

c. rpm-xfp11-l172 - remove interface Switch1.3172

d. rpm-xfp13-z074 - remove interface Switch1.4074

e. rpm-xfp04-l171 - remove interface Switch1.3171

- CSCsm72987

  Symptoms: When polling the ENTITY MIB for the gigabit ports that are integrated in the RSP720, there is an issue with entPhysicalParentRelPos for those Gigabit ports. They are reporting the same value.

  Conditions: Occurs on Cisco 7600 routers with the RSP720 card and running Cisco IOS Release 12.2(33)SRC and Cisco IOS Release 12.2(33)SRB1.

  Workaround: There is no workaround.

- CSCsm73592

  Symptoms: A reload may occur when an anything over MPLS (AToM) VC is torn down. Bug triggered initial crash of SIP-400 in slot 4 & ES20 in slot 3. Both cards had to be powered down and reset from the console to recover.

  Conditions: Occurs when AToM VC is setup and torn down later.

  Workaround: There is no workaround.

  Further Problem Description: The crash may occur when an event triggers access to a previously set up AToM VC. For example, the crash may occur when fast reroute (FRR) is configured on the tunnel interface and the primary interface is removed, such as in the following scenario:

  pseudowire-class ER1_to_HR1_EoMPLS no preferred-path interface Tunnel501331 disable-fallback ! interface tunnel501331 shutdown ! no interface tunnel501331

- CSCsm77171

  Symptoms: Router will crash.

  Conditions: Occurs with high traffic conditions where NetFlow has no free flows and multicast egress NetFlow is configured.

  Workaround: Disable multicast egress NetFlow.

- CSCsm79148

  Symptoms: SNMPwalk fails with packet too big error on enterprises.9.9.492 in the OID tree.

  Conditions: SNMPwalk failing with packet too big error.

  Workaround: Exclude the cermScalarsGlobalPolicyName SNMP object using a view as shown below: **snmp-server view testview internet included snmp-server view testview cermScalarsGlobalPolicyName excluded snmp-server community public view testview RO**

- CSCsm79995

  Symptoms: Spurious memory access may occur at line card which cause SIP-400 to crash.

  Conditions: May occur when attaching a service policy to any interface or removing the service policy.

  Workaround: There is no workaround.

- CSCsm87721

  Symptoms: Dialer Cisco Express Forwarding (CEF) with IP accounting fails with packet counters returning zero for the member interface.

  Conditions: This happens when **ip accounting output-packets** configured on NAS. The NAS is being checked for **show adjacency detail** which returns 0 packets and 0 bytes for the member interface.

  Workaround: There is no workaround.

- CSCsm89526

  Symptoms: When a new class-map configuration is added to policy-map, packet (which belongs to another existing class) drop issue will be observed.

  Conditions: Occurs on a Cisco 7600 router with ES20 and running Cisco IOS Release SW 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCsm89735

  Symptoms: A router might crash when the **show idb** command is issued.

  Conditions: The crash is seen when the **show idb** command is issued after a large number of PPPoE sessions (for example, 6000 sessions) are initiated and cleared. The crash is seen with IPv6, but it is not seen with IPv4.

  Workaround: There is no workaround.

- CSCsm92916

  Symptoms: When the number of VCs configured for out-of-band clock master are not continuous, the SPA might not generate packets for some of the clock master VCs.

  Conditions: Occurs on the following hardware:

  - SPA-24CHT1-CE-ATM
  - SPA-1CHOC3-CE-ATM
  - SPA-2CHT3-CE-ATM

  Workaround: Configure out-of-band clock master so that the number of VCs are continuous.

- CSCsm93088

Symptoms: After a flap or disconnection/restoration of T1s, random Multilink bundles on Cisco 7606 running Cisco IOS Release 12.2(33)SRB2 are up, but traffic does not pass through it when working with a third-party device.

Conditions: Problem of interoperatibility when working third-party device, the problem is present with the flap of T1 lines. When the T1s are restored, there is a problem with the synchronization on the sequence numbers.

Workaround: Delete and reconfigure again the bundle or reset the linecard.

- CSCsm96355

  Symptoms: A Cisco 7600 running a Cisco IOS Release 12.2SR image might experience a small amount of packet loss (about 10-20 ms) during TE-FRR reoptimization. This happens only for EVC (Ethernet Virtual Circuit) or scalable Ethernet Over MPLS (EoMPLS) configurations with large number of traffic engineering (TE) tunnels.

  Conditions: This issue happens only for traffic going over EVC or scalable EoM VCs when the box has scaled configuration, such as a large number of TE tunnels.

  Workaround: There is no workaround.

- CSCsm96785

  Symptoms: You may observe a problem which the OSPF neighbor is down after switch-over in spite of using OSPF Non-Stop Forwarding (NSF).

  Conditions: This occurs with the following conditions: - "nsf cisco" is only affected. If "nsf ietf", this problem does not occur. - You may observe this problem if the OSPF interface is "point-to-multipoint non-broadcast" or "point-to-multipoint". If the interface is "broadcast", this problem does not occur. - When this problem occurs after switch-over, DBD packet may not be exchanged between two neighbors. And the neighbor is down in spite of NSF.

  Workaround: Change the OSPF config to "nsf ietf" and change the OSPF interface to "broadcast".

- CSCsm97297

  Symptoms: Output direction ACL does not work.

  Conditions: Occurs when **ip cef accounting** is enabled on a MPLS enabled router doing tag disposition. If packets coming in are tagged, and they are going out of the router as untagged, the output IP ACL may not work.

  Workaround: Reconfigure the static route or clear the route.

- CSCso00793

  Symptoms: Enhanced-Flexwan crashes with cache error with MEM-CC-WAN-512M=, version "VI4DP647228EBK-MD" installed.

  Example of Symptom:

  ```
  Cache error detected! CP0_CAUSE (reg 13/0): 0x00004000 CPO_ECC (reg 26/0): 0x40000000
  Data cache error CPO_BUSERRDPA (reg 26/1): 0xFFDFFFE0 CPO_CACHERI (reg 27/0):
  0x200011C0 Tag address parity error Instruct cache index 0x0000008E CPO_CACHERD (reg
  27/1): 0x840000A0 Multiple data cache errors External cache error Data cache index
  0x00000005 CPO_CCHEDPA (reg 27/3): 0x09271600
  Interrupt exception, CPU signal 20, PC = 0xA0000100
  -Traceback= 40723DA8 406AF1B0 406B5BC8 406BAAF8 406BC200 406B4788 4072AA0C 4011D870
  4012D204
  ```

  Conditions: This issue is seen under certain conditions, which are not fixed. No specific trigger.

  Workaround: There is no workaround.

- CSCso06409

Symptoms: A Cisco 7600 (RSP720-3C/CXL) may experience high CPU utilization from the moment (S,G) expires due to all outgoing interfaces are down.

Conditions: This symptom occurs when indirect-connected multicast source traffic arrives at PIM-RP router without any receiver on that group, a (*,G) state with NULL RPF interface and NULL OIL is created and used to forward the traffic. Because of NULL RPF, this (*,G) state cannot be installed in Cisco 7600 hardware. The multicast data packet is punting to CPU and causes high CPU utilization.

Workaround: Partial workaround is to apply RP rate-limiter with fib-miss option.

- CSCso10596

  Symptoms: Polling cvpdnSessionAttrDevicePhyId from the CISCO-VPDN-MGMT MIB may show that multiple users are mapped to the same Virtual-Access SNMP ifIndex. This affects statistics collection or billing using IF-MIB counters.

  Conditions: This symptom is observed when PPP renegotiates an existing PPP connection on a Virtual-Access interface.

  Workaround: When possible, use RADIUS accounting for gathering statistics or billing.

- CSCso12305

  Symptoms: The IPv6 Cisco Express Forwarding (CEF) table may be missing prefixes which are present in the IPv6 RIB.

  Conditions: Occurs when CEF is disabled and re-enabled.

  Workaround: Enter the **clear ipv6 route *** command.

- CSCso15725

  Symptoms: Module's configuration not synchronized to standby supervisor if module resets while standby is booting up.

  Conditions: This bug may be seen if linecard or SPA were to reset before standby reaches standby hot terminal state.

  Workaround: Use **redundancy reload peer** to reset standby supervisor. On its next boot, configuration is synchronized to standby.

- CSCso20519

  Symptoms: There is some probability of Cisco IOS bootup failures on the Cisco 7600-SSC-400.

  Conditions: The failures are seen at cold temperature corners in testing. There are no failures reported from the field.

  Workaround: There is no workaround.

- CSCso21611

  Symptoms: Device crashes due to memory allocation issue.

  Conditions: Observed on Cisco 7200, but this is not a platform-specific bug.

  Workaround: There is no workaround.

- CSCso40678

  Symptoms: Multilink PPP interface may cease passing traffic after one of the MLP group's member links receives an AIS from the TDM network.

  Conditions: Problem occurs on a Cisco 7600/SUP-720/OSM/CHOC12/T1-S1 running the c7600s72033-adventerprisek9-mz.122-33.SRB2 image.

  Workaround: Perform a **shut/no shut** of the multilink interface.

- CSCso44120

  Symptoms: Unable to perform SNMPwalk of clcFdbVlanInfoTable.

  Conditions: Occurs all the time.

  Workaround: There is no workaround.

- CSCso49598

  Symptoms: Standby reloads continuously when "MAXINT" is used with "int ran" to create logical interfaces using.

  Conditions: Occurs in SSO mode.

  Workaround: Avoid giving MAXINT as range.

  Further Problem Description: At a stretch, only 1000 logical interfaces could be created through interface range. Due to some wrap-around problem, it was not showing error when MAXINT was given as option and starts creating these many interfaces which are much beyond the MAXINTERFACES supported by any existing platform. It will lead to MEMORY getting exhausted and different after effects as standby reload.

- CSCso50602

  Symptoms: Router reloads after the **show ip bgp ipv4 mdt vrf** command is entered.

  Conditions: Occurred on a Cisco 7600 router running Cisco IOS Release 12.2(33)SRB2. Occurs when the **show ip bgp ipv4 mdt vrf** command entered with the *ip address* option, such as **show ip bgp ipv4 mdt vrf abc123** *x.x.x.x*.

  Workaround: The reload can be avoided by not using the IP address option with the 'show ip bgp ipv4 mdt vrf' command. None of the other options available for this command will trigger a reload

- CSCso53306

  Symptoms: A Cisco IOS device may crash with a data bus error exception and stack trace PC = 0xA0000100

  Conditions: Device is running normal production traffic. Presence of malformed punted RP packets in this network caused the issue.

  Workaround: There is no workaround.

- CSCso53377

  Symptoms: With large number of label switched paths (LSP), the SSO recovery process may take longer than expected. Therefore sometimes not all traffic engineering (TE) LSPs can recover after SSO switchover.

  Conditions: Occurs on when there is a large number of LSPs.

  Workaround: There is no workaround.

- CSCso54167

  Symptoms: BGP peers are struck with table versions of 0. BGP peers do not announce any routes to neighbors.

  Conditions: Whenever the interfaces are flapped with online insertion and removal (OIR) multiple times, all of the BGP peers using such interfaces for peering connections encounter this issue.

  Workaround: Delete and reconfigure the neighbor.

- CSCso56185

Symptoms: L2TP Start-Control-Connection-Reply (SCCRQ) and Start-Control-Connection-Reply (SCCRP) messages have incorrect setting of mandatory-bit for the receive window Size attribute-value pair (AVP). This may cause L2TP/VPDN sessions to fail to connect.

Conditions: Occurs in VPDN environments where the peer requires tight protocol adherence.

Workaround: There is no workaround.

- CSCso57886

  Symptoms: A Cisco IOS device may crash with a data bus error exception and stack trace PC = 0xA0000100

  Conditions: Device is running normal production traffic. Presence of malformed punted RP packets in this network caused the issue.

  Workaround: There is no workaround.

- CSCso62526

  Symptoms: Standby supervisor reloads after the interface configuration command **no flow-sampler <name>** is used to remove flow sampler map.

  Conditions: Occurs on a Cisco 7606s with two RSP720-3C-GE configured for normal use with sampled NetFlow configured. To cause the issue, a sampler must be explicitly detached.

  Workaround: There is no obvious workaround to the issue. To avoid the issue, avoid detaching the sampled NetFlow.

- CSCso63263

  Symptoms: The RP will start showing IPC-5-WATERMARK: 988 messages pending in xmt for the port messages on the screen. The number of messages will change.

  Conditions: The router has 275,000 i-BGP routes injected into the router. Among these routes, 100,000 are flapped continuously for one to one and half days. They are flapped every 10 sec. The problem needs at least a days worth of time of continuous flapping.

  Workaround: Stop the route flap. Although the messages will keep coming, there is no impact on functionality. And they are bogus since they are originated from wrong count.

- CSCso63807

  Symptoms: Packet loss when pinging an IP Address in a VPN routing/forwarding (VRF).

  Conditions: This problem is seen on a Cisco 7600 after the VRF configuration on a port is rapidly changed, such as the following example:

  ```
  interface gi3.1.88 ip vrf forwarding aaaa ip vrf forwarding bbbb
  ```

  Workaround: Delete the VRF with **no ip vrf forwarding aaaa** before changing the VRF under the interface.

  Further Problem Description: The VLAN RAM, which stores the VRF ID, is programmed wrong when this issue is seen. This causes packet loss or packets to be punted to the RP to resolve the conflict

- CSCso66668

  Symptoms: FlexWAN line card crashes in Cisco 7600 chassis.

  Conditions: Occurs when bre-connect is configured on an ATM PVC.

  Workaround: There is no workaround.

- CSCso66862

  Symptoms: Router crashes due to bus error. The crash is seen after repeatedly removing virtual-template interfaces under ATM.

Conditions: The crash is seen under the following conditions.

1) Bringing up nearly 3k PPPoE and PPPoEoA sessions.

2) Configuring **no interface virtual-template <no>** under ATM interfaces.

Repeating Step 2 continuously will cause a crash.

Workaround: There is no workaround.

- CSCso78716

  Symptoms: SNMP object entPhysicalVendorType returns incorrect value.

  Conditions: Occurs only on a Cisco 7603s.

  Workaround: There is no workaround.

- CSCso79720

  Symptoms: When the **show interface** command is entered , all of the Layer 2 swith port interfaces on ES-20 are shown with the same bridge MAC.

  Conditions: Only seen on ES-20.

  Workaround: There is no workaround.

- CSCso86674

  Symptoms: Border Gateway Protocol (BGP) is unable to get route information after **shut/no shut** is performed on BGP neighbor on far-end.

  Conditions: Issue is seen when BGP is used for IPv6 routing.

  Workaround: This problem can be recovered by doing shut and no-shut again. Also, problem will not happen if you set network <prefix> at address-family on far-end router.

- CSCso87348

  Symptoms: A Catalyst 6500 or a Cisco 7600 may reload unexpectedly.

  Conditions: Occurs when NetFlow is configured on one of the following:

  - Cisco 7600 running Cisco IOS Release 12.2(33)SRC.
  - Catalyst 6500 running Cisco IOS Release 12.2SXH.

  Workaround: Disable Netflow. This is done with the following commands: no ip flow ingress no ip flow engress no ip route-cache flow Enter the appropriate command for each sub-interface for which NetFlow is currently configured.

- CSCso88898

  Symptoms: The line card displays memory allocation failure messages, and memory statistics indicate a continuous decline in free memory.

  Conditions: When port mode or VC mode cell relay configuration is applied on an ATM interface, it is observed that after traffic switching for a long time (approximately 48 hours, depending on scale), the above problem occurs.

  Workaround: There is no workaround.

- CSCso91230

  Symptoms: A router may display the following error: %LINK-2-INTVULN: In critical region with interrupt level=0, intfc=ATM0 -Process= "IGMP Snooping Receiving Process"

  Conditions: The symptom is observed when bridged traffic is passing to an MLPP interface.

  Workaround: Disable IGMP snooping with the **no ip igmp snooping** command.

- CSCso93883

  Symptoms: Upon reload of a DFC, traffic coming from the MPLS cloud might be dropped when the traffic is destined for a EoMPLS connection on a MUX-UNI

  Conditions: This is seen on 12.2(33)SRB3 and 12.2(33)SRA3. The incoming module needs to be a DFC, and the egressing port needs to be a MUX-UNI. This does not happen to regular Ethernet Over MPLS (EoMPLS) connections.

  Workaround: Perform a **shut/no shut** on the connection towards the MPLS network, then **shut/no shut** the VC.

- CSCso99860

  Symptoms: Some of the initially shipped PWR-1500-DC power supplies in Cisco 7603S chassis have incorrect SNMP OID programmed in the IDProm. The vendorOID does not match with the CANA-assigned number in CISCO-ENTITY-VENDORTYPE-OID-MIB.my

  Conditions: This is applicable for those power supplies for which the vendorOID is programmed as 193 and not as 194.

  Workaround: There is no workaround.

- CSCsq09962

  Symptoms: Cisco 7600 router crashes at "pim_proxy_empty_rd."

  Conditions: Customer seeing crash with decode during initial deployment of new Cisco 7600 router.

  Workaround: There is no workaround.

- CSCsq13938

  Symptoms: In Cisco IOS software that is running the Border Gateway Protocol (BGP), the router may reload if BGP **show** commands are executed while the BGP configuration is being removed.

  Conditions: This problem may happen only if the BGP **show** command is started and suspended by auto-more before the the BGP-related configuration is removed, and if the BGP **show** command is continued (for example by pressing the SPACE bar) after the configuration has been removed. This bug affects BGP **show** commands related to VPNv4 address family. In each case the problem only happens if the deconfiguration removes objects that are being utilized by the **show** command. Removing unrelated BGP configuration has no effect.

  This bug is specific to MPLS-VPN scenarios (CSCsj22187 fixes this issue for other address-families).

  Workaround: Terminate any paused BGP **show** commands before beginning operations to remove BGP-related configuration. Pressing "q" to abort suspended show commands, rather SPACE to continue them, may avoid problems in some scenarios.

- CSCsq16830

  Symptoms: Stale NFS entry left on ESM20G card when diagnostics is enabled.

  Conditions: Occurs on Cisco 7609 ESM20G cards after the router is reloaded.

  Workaround: Disable diagnostics and reset the line card.

- CSCsq19146

  Symptoms: Customer seeing multiple "%SIP200_SPIRX-3-SPA_INTERRUPT: SPA 0 - seq err, SPA Int status = 0x4" errors.

  Conditions: Occurs under normal operating conditions.

  Workaround: There is no workaround.

- CSCsq19159

Symptoms: System crash or memory corruption occurs.

Conditions: Occurs when repeated linecard resets are seen in the device or repeated linecard online insertion and removal (OIR) operations are performed.

Workaround: There is no workaround.

- CSCsq20970

  Symptoms: On the 2432 platform UUT, the 'atm' option is missing in the 'mode' CLI when the T1 controller is being configured for ATM.

  Conditions: The symptom is observed on the 2432 platform with a T1 controller.

  Workaround: There is no workaround.

- CSCsq22383

  Symptoms: A Cisco 7600 router may sometimes hang while performing configuration/deconfiguration stress tests

  Conditions: Occurs on a Cisco 7600 router running Cisco IOS Release 12.2(33)SRB3.

  Workaround: There is no workaround.

- CSCsq22417

  Symptoms: A Cisco 7600 running configuration/deconfiguration tests repeatedly over time may crash.

  Conditions: Unknown conditions.

  Workaround: There is no workaround.

- CSCsq25028

  Symptoms: Malloc errors seen on enhanced FlexWANs with 256MB memory in RSP720 systems when another line card is inserted or powered up. FlexWAN I/O memory low watermark becomes very low while number of allocated IPC buffers grow in the hundreds.

  Conditions: Seen only on RSP720, not seen on SUP720 systems. Routing table has 30,000 routes or more.

  Workaround: There is no workaround.

  Further Problem Description: Inserting or powering up a line card prompts the RP to send all info to all cards and FlexWAN bays in chassis. RSP720 sends info at higher rate than FlexWAN can immediately process, so hundreds of IPC buffers are allocated until its I/O pool is exhausted and malloc error reported. May not impact operation, but risk of memory fragmentation and other failures increase.

- CSCsq31808

  Symptoms: With eiBGP multipath, incoming labeled packets may get looped in MPLS core instead of getting forwarded to CE, causing traffic issues. The following symptom may be found:

  – The error message below is frequently generated.

    ```
    Dec 17 07:44:46.734 UTC: %COMMON_FIB-3-BROKER_ENCODE: IPv4 broker failed to encode
    msg type 0 for slot(s) 0B -Traceback= 6044E470 60465864 6043BCFC 6043B570
    ```

  – The **debug cef xdr** command yields the following message:

    ```
    Mar 31 17:44:40.576 UTC: FIBrp_xdr: Table IPv4:<vrf name>, building insert event
    xdr for x.x.x.x/y. Sources: RIB Mar 31 17:44:40.576 UTC: FIBrp_xdr: Encoding path
    extensions ... Mar 31 17:44:40.576 UTC: FIBrp_xdr: - short ext, type 1, index 0
    Mar 31 17:44:40.580 UTC: FIBrp_xdr: Getting encode size for IPv4 table broker
    ```

```
FIB_FIB xdr Mar 31 17:44:40.580 UTC: - short path ext: len 12 Mar 31 17:44:40.580
UTC: - short path ext: len 24 Mar 31 17:44:40.580 UTC: - feat IPRM, len 12 Mar 31
17:44:40.580 UTC: => pfx/path 113 + path_ext 24 + gsb 8 + fs 16 = 161
```

– Checking the prefix, it point to drop entry.

```
router#show mpls forward vrf <vrf name> x.x.x.x Local Outgoing Prefix Bytes Label
Outgoing Next Hop Label Label or VC or Tunnel Id Switched interface 937 No Label
x.x.x.x/y[V]  0 drop <========= it is drop
```

– Checking the MOI flag of EBGP path, the No_Global flag (0x10) was incorrectly set

```
router#show ip cef vrf <vrf name> x.x.x.x int [snip] path_list contains at least
one resolved destination(s). HW not notified path 70BFFC5C, path list 20E87B58,
share 1/1, type recursive nexthop, for IPv4, flags resolved MPLS short path
extensions: MOI flags = 0x16 <-------MOI flags 0x10 is incorrectly set (for ebgp
path, correct flag should be 0x4, 0x5, 0x6 ..) correct now. [snip]
```

Conditions: eiBGP multipath enalbed; iBGP path comes up first , then the eBGP path. Both eBGP & iBGP paths could be in MPLS forwardinging casuing the issue.

Workaround: Using the **clear ip route vrf <name> x.x.x.x** clears the issue.

- CSCsq31923

  Symptoms: Crash may occur after polling MPLS-LSR-MIB mplsInterfaceConfTable.

  Conditions: MPLS-enabled tunnels exist in configuration and some are removed by doing **no int tunnel<tunnelid>**. If mibwalk of any object in mplsInterfaceConfTable is performed after that, this may result in crash.

  Workaround: Remove MPLS configuration on tunnel with the **no tunnel mode mpls traffic-eng** command before entering the **no int tunnel** command.

  Further Problem Description: It has been found this problem occurs when tunnel also contains the following config: **tunnel mpls traffic-eng path-option 1 dynamic**. Crash occurs only if image contains fix for CSCsm97259. Will see this message similar to the following before the crash:

  ```
  Jun 3 11:53:59.955 PDT: %TIB-3-GENERAL: MPLS MIB subblock ifIndex corrupted for
  ifIndex: 46 - was: 1198404176; corrected
  ```

- CSCsq36782

  Symptoms: In Ethernet Over MPLS (EoMPLS) enviroment after fast reroute (FRR) from interface on SIP600 to interface on SIP400 and re-optimization, traffic is blackholed from CPE device to core.

  Conditions: This happen only after FRR from SIP600 module to SIP400 module. FRR between SIP400 does not experience this problem.

  Workaround: There is no workaround.

- CSCsq42931

  Symptoms: Cisco 7600 series of router may reload twice when the router is booting up.

  Conditions: This is a very rare occurrence. A Cisco 7600 series might reload while it is booting up. Additionally, spurious access might be seen when linecards are booting up. These messages have no impact on functionality or stability of the router.

  Workaround: There is no workaround.

- CSCsq43831

  Symptoms: A Cisco IOS router may unexpectedly reload when Forwarding Information Base (FIB) processes an adjacency for route that has many levels of recursion.

  Conditions: This has only been seen after the following error message was displayed:

  ```
  %COMMON_FIB-6-FIB_RECURSION: 10.10.10.1/32 has too many (8) levels of recursion during
  setting up switching info
  ```

Workaround: Change static routes so they specify both the interface and next-hop instead of just specifying the next-hop. For example change:

ip route 10.0.0.0 255.255.255.255 192.168.1.1

to

ip route 10.0.0.0 255.255.255.255 GigabitEthernet1/0 192.168.1.1

This is particularly true when using eBGP between loopbacks to allow for multiple parallel links between the two eBGP peers, where one typically installs static routes for the eBGP peers address. Make sure these static routes have both interface and next-hop specified.

- CSCsq47355

  Symptoms: On Cisco 7600 routers, the switch processor may crash the router when BGP is configured in rare situations.

  Conditions: This is a rare condition that can can most likely happen with L3VPN and BGP recursive routes configured when a network, routing, or link event occurs (e.g., link flap in the remote ends, routing flaps, etc). This issue may also require routes to be load-balanced over multiple links.

  This issue only affects 12.2(33)SRB and 12.2(33)SRC and is fixed in 12.2(33)SRB4 and 12.2(33)SRC2 and later releases.

  Workaround: There is no workaround.

- CSCsq57462

  Symptoms: Ethernet Out of Band Channel (EoBC) hang causes line card reset. EoBC might get stuck resulting in communication loss between RP/SP and line card. This will result in line cards getting reset. This is a very rare condition and is seen only once so far.

  Conditions: Occurs during increased EoBC traffic due to convergence or link flap and is very rarely seen.

  Workaround: This impacts only one CPU. A forced switchover will recover from this condition.

- CSCsq62703

  Symptoms: Intermediate System-to-Intermediate System (IS-IS) tries to access invalid memory address and may cause router to stop working.

  Conditions: Occurs when a switch over happens and standby router becomes active.

  Workaround: There is no workaround.

- CSCsq67779

  Symptoms: Port numbering is incorrect during SNMPwalk. For example, PORT 3/1/3 is displayed as 3/0/13.

  Conditions: This is seen during SNMPwalk of ES20 line cards.

  Workaround: There is no workaround.

- CSCsq67811

  Symptoms: System crashes due to I/O memory with the following error message:

  ```
  "%ETSEC-3-RECOVER_TX: Interface EOBC0/0 TX workaround invoked"
  ```

  Conditions: This condition is caused by a lockup inside the Ethernet Out of Band Channel (EOBC) MAC. This problem is rarely seen.

  Workaround: There is no workaround.

- CSCsq67817

  Symptoms: ETSEC freeze might cause router to crash due to memory depletion.

Conditions: There is a rare hardware issue, which might lock up ETSEC driver transmit. This condition has been observed only once.

Workaround: There is no workaround.

- CSCsq71036

  Symptoms: On Cisco 7600 routers, a possibility exists of various error messages being seen due to memory corruption.

  Conditions: No known triggers. The error has never been reported on a Cisco 7600 router, only on Cisco 6000 routers.

  Workaround: There is no workaround.

- CSCsq87496

  Symptoms: "%OIR-6-INSCARD" syslog event is not sent from the device following online insertion and removal (OIR).

  Conditions: Occurs after a card has been inserted. "%OIR-6-INSCARD: Card inserted in slot x, interfaces are now online" syslog message should be sent, but is not.

  Workaround: Use SNMP to trap "entconfigchange".

- CSCsq88905

  Symptoms: ES-20 ports are not properly modeled in CiscoActive Network Abstraction (Cisco ANA). Some ports snmp-presentation locations are shown incorrectly.

  Conditions: The issue is seen when ANA is used to manage ES20 line card.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRB3

Cisco IOS Release 12.2(33)SRB3 is a rebuild release for Cisco IOS Release 12.2(33)SRB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRB3 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCdv07156

  Symptoms: A router that is configured with thousands of RIP routes may crash when multiple links flap.

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

  Workaround: There is no workaround.

- 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
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa


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:

Configuring Authorization:

http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/12_4/sec_secure_connectivity_12_4_book.html

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#wpxref9538

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#wp480029

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

- CSCed88426

  Symptoms: An extended ACL applied on an interface does not permit/deny traffic as expected on the standby after switchover.

  Conditions: This symptom occurs when the user does ACL configuration using acl submode and types Ctrl-C. This causes the config mode to be exited on active, but the command line synced to standby is "\0". Nothing gets executed on standby, and the ACL submode exit handler is not called. If switchover happens, ACL configuration becomes out of sync.

This happens only at the first switchover. Subsequent switchovers do not show this issue.

Workaround: Avoid the use of Ctrl-C in the ACL submode, instead use Ctrl-Z or **exit** command.

- CSCef15846

  Symptoms: There are two symptoms which are fixed by this bug.

  Symptom 1: When the last peer of a peer-group that is defined in a vrf address- family is deleted, the peer-group configuration will also disappear if no policy is configured for the peer-group.

  Condition 1: This symptom is observed in a customer configuration modification.

  Workaround 1: Configure a policy for the peer-group such as a route-map.

  Symptom 2: Peer-group that is used exclusively by IPv6 peers is activated under the IPv4 address-family.

```
sho configuration  | b address-family ipv4
    address-family ipv4
    neighbor rr-server activate
    neighbor RD-BGP-SOURCE activate
    neighbor v6-rr-server activate <==
    neighbor 10.1.1.1 peer-group rr-server
    neighbor 10.1.1.2 peer-group rr-server
    neighbor 192.168.1.1 peer-group RD-BGP-SOURCE
    no auto-summary
    no synchronization
    exit-address-family
```

  Condition 2: This symptom is observed when the v6 peer-group is activated under the IPv4 address family as soon as it is created.

  Workaround 2: There is no workaround.

- CSCeg52893

  Symptoms: VTY or TTY sessions may hang after unsuccessful authentication attempts to an external AAA server. For a line that is still considered active, the output of the **show line** *line-number* command, shows the following:

```
Modem state: Ready, Carrier Dropped
```

  When you enable the **debug tacacs** command, the following debug statement is generated during the authentication failure:

  No sock_ctx found while handling request timeout

  Conditions: This symptom is observed on a Cisco platform when external authentication fails before the maximum authentication attempts are reached locally.

  Workaround: When the symptom has occurred, reload the router to clear the hung VTY or TTY sessions. For a NAS with internal modems, you may be able to clear the hung VTY or TTY sessions by entering the **clear port** *slot/port* EXEC command.

  To prevent the symptom from occurring, configure the maximum authentication attempts on the Cisco platform to be lower than the maximum authentication attempts on the external AAA server by entering the **aaa authentication attempts login** *number-of-attempts* global configuration command, in which the *number-of-attempts* argument is a value that is smaller then the maximum authentication attempts that are configured on the external AAA server.

- 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.

- CSCej77184

  Symptoms: After an SSO switchover has occurred, the following error message may be generated:

  ```
  LSD-4-LABEL_RESOURCE: label range 16-524287 exhausted
  ```

  Conditions: This symptom is observed on a Cisco router that functions in an MPLS configuration under a heavy traffic load that causes bulk synchronization to take a relatively long time. The symptom occurs when there is label allocation between the “bulk-sync-done” state and the “Standby Hot” state.

  Workaround: There is no workaround.

- CSCek73579

  Symptoms: Site of Origin (SoO) filtering appears broken and allows unexpected entries.

  Conditions: This symptom is seen during normal use.

  Workaround: There is no workaround.

- CSCek73767

  Symptoms: Reloading Gigabit Ethernet SPA causes a line card to crash.

  Conditions: This symptom has been observed when the **hw-module slot 0/0 reload** command is entered and then the line card in slot zero crashed.

  Workaround: There is no workaround.

- CSCek76062

  Symptoms: A router crashes because of a block overrun (overwriting the memory block).

  Conditions: This symptom is observed only when templates are exported in the export pak, which is used only in version 9 version of exporting.

  Workaround: Version 5 could be used for exporting.

- CSCek76602

  Symptoms: There is a rare possibility that the console may stay with RP after the system crashes and does not switch to SP. If the system is not configured with autoboot, it might look like a hang state.

  Conditions: This symptom happens when RP crashes first and then SP gets exception while creating crashinfo file. Not easily reproducible. Problem is seen after multiple switchover [Number of switchovers is not predictable].

  Workaround: Router power recycle is required.

- 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**.

- 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:

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

- CSCsb06069

  Symptoms: The primary becomes very slow when accepting CLI commands after the user executes **rtr reset** or any **rtr** command, which requires human interaction.

  Conditions: This symptom happens when there is a SSO setup.

  Workaround: Do not execute **rtr** commands, which require human intervention.

- CSCsb36463

  Symptoms: IGMP packets are rate limited when they arrive on a layer 3 port (routed port) and are sent to the route processor.

  Conditions: The IGMP packets can be rate-limited if (1) IP-option rate limiter is configured using the **mls rate-limit multicast ip-options** *pps packets-in- burst* command, and IGMP packets contain router alert option. (2) FIB miss rate limiter is configured using the **mls rate-limit multicast ipv4 fib-miss** *pps packets-in- burst* command.

  Workaround: Configure ports as switchports with an SVI instead of a routed port or increase rate limiter parameters to allow expected level of IGMP packets.

- CSCsb93068

  Symptoms: WS-x6148-FE-SFP shows incorrect value in CISCO-STACK-MIB::PortTable when SFPs are inserted.

  PortType shows as e100baseEmpty when SFPs are inserted.

Conditions: This symptom occurs in Cisco 6500 that is running Cisco IOS Release 12.2(18)SXF with WS-x6148-FE-SFP card. Does not have support for the new 100BASE SFPs and there is no Functional impact.

Workaround: There is no workaround.

- CSCsc75381

  Symptoms: Native VLAN mismatch may not be detected when native VLAN is not consistent on two ends of 802.1Q trunk and native VLAN is not allowed on one end only. This is a case of misconfiguration, but it may result in a forwarding loop.

  For example:

  ```
  switch1(native=3)---802.1Q_trunk---(native=2)switch2


  allowed vlans on switch1: 3,4
  allowed vlans on switch2: 3,4
  ```

  If STP designated port is on the switch1 side, this misconfiguration may not be detected.

  Conditions: This symptom occurs when misconfiguration is not detected.

  Workaround: Correct misconfiguration. Make native VLAN consistent on both sides or at least allow VLAN 2 (native) on trunk on switch2.

- CSCsc98835

  Symptoms: OSPF and BGP change their state unexpectedly.

  Conditions: This symptom is observed on a Cisco router when a modification of a shared access control list (ACL) that is called from more than 300 route maps causes a CPUHOG condition in the Virtual Exec Process.

  Workaround: There is no workaround.

- CSCsd36094

  Symptoms: Multiple duplicate system error messages are seen.

  Conditions: This symptom is observed when duplicate system ID is configured on multiple IS-IS instances in the same VRF.

  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.

- CSCsd77622

  Symptoms: The **show policy-map interface** command is not showing the exceeded and violated counters.

  Conditions: This symptom happens only when trust is enabled in the policy-map.

Workaround: There is no workaround.

- CSCsd88768

  Symptoms: With PPP multilink configured on serial links on PA-MCX-8TE1, the following error message may be seen:

  ```
  %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=3, count=0
  ```

  Conditions: With PPP multilink configured on serial links on PA-MCX-8TE1 and when traffic is flowing, the following error message may be seen:

  ```
  %SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=3, count=0
  ```

  Workaround: There is no workaround.

- CSCsd93294

  Symptoms: On a CSC-PE router with dual RPs, the following is seen on the standby RP:

  1. A near endless amount (about 45-50) of the following error messages:

  ```
  00:34:51: %FRR_OCE-STDBY-3-GENERAL: Primary interface number and OCE do not
   match.
   -Traceback= 42519710 4251A080 425010D4 4250176C 42527400 416E7DDC 416E83E8
   416E9270 41768BD8 4194E404 421DCA90 41958978 41959080

   00:34:51: %SYS-STDBY-2-CHUNKFREE: Attempted to free nonchunk memory, chunk
   531555D8, data 531554E0.
   -Process= "XDR LC Background", ipl= 2, pid= 131
   -Traceback= 412EFB3C 412EFE8C 42519588 42527740 416E7DDC 416E83E8 416E9270
   41768BD8 4194E404 421DCA90 41958978 41959080
  ```

  2. Followed immediately by a crash.

  Conditions: This symptom occurs when performing an SSO switchover.

  Workaround: There is no workaround.

- CSCse03637

  Symptoms: PIM dense mode interoperability issues are seen with Cisco and third party boxes.

  Conditions: This symptom is observed when PIM dense mode is in operation. After the multicast forwarder is decided, based on the assert mechanism, a prune is erroneously sent. Multicast stream ceases to flow.

  Workaround: There is no workaround.

- CSCse65277

  Symptoms: Standby reloads due to default ISIS metric maximum returns parser error.

  Conditions: This issue is observed while configuring the ISIS metric maximum on an interface by using the **isis metric maximum** command and later changing it in to the default metric value.

  Trigger: At this point, it will show the error, and the communication with the peer Supervisor has been lost then the standby reloads.

  Workaround: There is no workaround.

- CSCsf06946

  Symptoms: After you have removed a loopback interface from the configuration on the primary RP while the same loopback interface is required as part of another configuration, for example, as an update source for a BGP neighbor, the standby RP does not reload successfully when you reset it.

Conditions: This symptom is observed on a Cisco router and occurs only in an HA environment.

Workaround: Remove all configurations that reference the loopback interface before you remove the loopback interface.

- CSCsf96980

  Symptoms: IPv6 multicast traffic fails to be forwarded after a second SSO failover.

  Conditions: This problem is extremely intermittent with no discernible triggers.

  Workaround: There is no workaround.

- CSCsg07870

  Symptoms: The new active supervisor engine may crash after an SSO switchover has occurred.

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

  Workaround: There is no workaround.

- CSCsg24971

  Symptoms: A memory leak may occur on a line card, eventually causing IPC to fail.

  Conditions: This symptoms is observed on a Cisco platform that is configured for NetFlow. The symptom affects distributed platforms only.

  Workaround: There is no workaround.

- CSCsg29305

  Symptoms: Router crashes when reloading a VPNSPA blade.

  Conditions: The problem shows after running all five devtests specific test suites. Running any one test suite will not cause this problem. The configuration generated by those test suites will not cause the problem either. The trigger of the combined actions is unknown at this point.

  Workaround: There is no workaround.

- CSCsg35077

  Symptoms: A device running Cisco IOS may crash during processing of an Internet Key Exchange (IKE) message.

  Conditions: The device must have a valid and complete configuration for IPsec. IPsec VPN features in IOS that use IKE include Site-to-Site VPN tunnels, EzVPN (server and remote), DMVPN, IPsec over GRE and GET VPN.

  Workaround: Customers that do not require IPsec functionality on their devices can use the command “no crypto isakmp enable” in global configuration mode to disable the processing of IKE messages and eliminate device exposure.

  If IPsec is configured this bug may be mitigated by applying access control lists that limit the hosts or IP networks that are allowed to establish IPsec sessions with affected devices. This assumes that IPsec peers are known. This workaround may not be feasible for remote access VPN gateways where the source IP addresses of VPN clients are not known in advance. ISAKMP uses port UDP/500 and can also use UDP/848 (the GDOI port) when GDOI is in use.

  Further Information: This bug is triggered deep into the IKE negotiation, and an exchange of message between IKE peers is necessary.

  If IPsec is not configured then it is not possible to reach the point in the IKE negotiation where the bug exists.

- CSCsg62154

Symptoms: The following traceback appears in the standby after SSO switchover.:

```
"SP-STDBY: ltl_alloc_index_at: LTL index(0x80A) in the permanent region already
allocated "
```

Conditions: The problem happens every time after SSO switchover and when the new standby supervisor has come up. This problem happens specifically with respect to ICROIF indices.

Workaround: There is no workaround.

- CSCsg87290

  Symptoms: When you enter the **shutdown** command followed by the **no shutdown** command on the SONET controller of a 1-port channelized STM1/OC3 to DS0 SPA (SPA-1XCHSTM1/OC3), an extra flap occurs for T3 links that are configured on the SONET controller.

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

  Workaround: There is no workaround.

- CSCsh05821

  Symptoms: BFD adjacencies will not form for EIGRP neighbors over interfaces defined in VRFs.

  Conditions: This symptom is seen in normal EIGRP/BFD configurations. This bug removes the restriction on using EIGRP/BFD over a VRF interface.

  Workaround: There is no workaround.

- CSCsh12493

  Symptoms: After addition/deletion/modification of a VRF and the re-addition of associated configuration, it becomes apparent that the RIB is not being updated by BGP after reconvergence, and LDP neighborship is reestablished. As the RIB is not updated, neither is CEF. While BGP VPNv4 has the correct information, the RIB is empty of remote PE VRF subnets, and CEF has a default entry.

  Conditions: This symptom is observed on Cisco 12000 series router that is running Cisco IOS Release 12.0(32)S6.

  Workaround: Can be recovered by clearing BGP session.

- CSCsh15817

  Symptoms: IP SLA operations on a router that has a response time reporter (RTR) enabled may fail at the source. The UDP socket events are not received by the RTR responder process, and the UDP socket events are missing when a UDP packet is routed through a VRF.

  Conditions: These symptoms are observed on a Cisco router that runs Cisco IOS Release 12.2SB. You can verify that the symptoms are occurring through any of the following commands:

  - **debug rtr trace**
  - **debug ip udp**
  - **debug socket**

  Workaround: Use IP SLA operations without VRFs.

- CSCsh17035

  Symptoms: A route may flap continuously, and the CPU usage may be high continuously.

  Conditions: This symptom is observed on a Cisco router that is configured with a static route loop.

  Workaround: Do not configure a static route loop.

- CSCsh17630

  Symptoms: In a dual RP system that is running in SSO mode, standby could be reset by the active if some invalid commands followed by valid commands are executed.

  Conditions: This symptom is seen in a dual RP system that is running in SSO mode. If invalid commands such as invalid interface commands are executed followed by valid commands, which are present in sub-configuration mode as well as in global configuration mode like the **mpls ip** command, which is present in interface configuration mode as well as in global configuration mode, then the standby could get reset by the active due to PRC failure on execution of such commands.

  Workaround: Do not configure invalid commands followed by valid commands which are valid in multiple configuration modes.

- CSCsh20140

  Symptoms: A small memory leak may occur when ISPF is enabled. When you deconfigure OSPF, the following error message and traceback are generated:

  ```
  %SYS-2-CHUNKPARTIAL: Attempted to destroy partially full chunk, chunk
  30E3268.
  -Process= "Exec", ipl= 0, pid= 3,
  -Traceback= 0x69F968 0x813670 0x8137C4 0xD57928 0xD6A230 0xB37824 0xB38550
  0x6E33F0 0x706EBC 0x7ABDD0 0x7ABDCC
  ```

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCsb38978. A list of the affected releases can be found at http://tools.cisco.com/Support/BugToolKit/search/getBugDetails.do?method=fetchBugDetails&bugId=CSCsb38978 Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: Do not configure ISPF.

- CSCsh33518

  Symptoms: When STP is configured on a Cisco Catalyst 6500 switch with Active and Standby SUP the **show spanning tree** command on the Standby SUP may show different information from that of Active SUP.

  For example:

  ```
  Active SUP xs6k3#sh spanning-tree
  VLAN0002
       Spanning tree enabled protocol ieee
       Root ID    Priority    32768
                  Address     0014.1bc4.c002
                  Cost        4
                  Port        259 (GigabitEthernet3/3)
                  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

       Bridge ID  Priority    32768
                  Address     0014.1bc4.f802
                  Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
                  Aging Time 15

     Interface           Role Sts Cost      Prio.Nbr Type
     ------------------- ---- --- --------- -------- --------------------------
  ```

```
-
 ---
   Gi3/3               Root FWD 4         128.259  P2p
   Gi3/4               Altn BLK 4         128.260  P2p

   xs6k3#


   Spanning Tree info on Standby
   -----------------------------
   xs6k3-sdby#sh spanning-tree

   No spanning tree instance exists.

   xs6k3-sdby#
```

Conditions: This condition is generic for Cisco IOS Release 12.2(18)SXF6 and earlier releases.

Trigger: This problem is due to the different load conditions on the Active and Standby SUP.

Impact: No spanning tree instance exists on standby.

Workaround: Manually reset Standby SUP to re-sync STP states from Active to Standby. However the STP states may digress again going forward.

Further Problem Description: This problem is due to the different load conditions on the Active and Standby SUP. Occasionally the Standby SUP may run ahead of Active SUP in terms of sync state. When there is a surge of activities on the Active SUP it may run behind the sync request/event coming from the Standby. When the sync event arrives too early the Active SUP drops the request due to wrong state/event combination and therefore the sync never happened and hence the discrepancy.

A fix is put in place to avoid this type of sync race condition between Active and Standby.

- CSCsh42678

  Symptoms: A standby Route Processor continuously reloads.

  Conditions: This symptom is observed when the **issu runversion** command is executed in a redundant router.

  Workaround: There is no workaround.

- CSCsh45949

  Symptoms: SAs are created by the crypto engine in the wrong subslot.

  Conditions: The crypto engine <slot>/<subslot>, when used on a different subslot, does not have an effect.

  For example, applying the **crypto engine slot** *2/1* command does not take effect (in the sense that the **show** command still displays that the old sub-slot 2/0 is in use instead).

  BUT when the traffic is sent the output of the **sh cry eli** command shows that the SAs are created using the crypto engine at 2/1 as opposed to 2/0 as shown in the configuration. Also all the traffic is sent to crypto engine at 2/0, and no traffic reaches 2/1. There is packet drop shown in the crypto engine at 2/0 as “Invalid SA”.

Workaround: Apply the **no crypto engine** *slot/sub- slot* command on the subslot on which it is to be disabled. Apply the **crypto engine** *slot/sub-slot* command on the new subslot on which this has to be enabled.

- CSCsh52567

  Symptoms: A Cisco RSP720 crash is experienced when BGP is established over SPA-1XOC12-POS interface where the problem is seen in Cisco IOS Release 12.2(33) SRB2.

  Conditions: This symptom is observed when BGP speaker is originating a prefix with an outbound routemap having *routemap continue* keyword and **set as-path prepend** in the routemap policy, under certain corner conditions, the router may reload.

  Workaround: In the BGP route map policy, remove the routemap *continue* keyword and change the policy logic when it is used along with routemap **set aspath prepend** command. Note that once routemap *continue* is removed, please make sure that the polices are changed such that they are similar to the originally intended policy behavior.

- CSCsh54797

  Symptoms: This issue causes high CPU utilization.

  Conditions: This issue occurs with PPPoE sessions. When bringing up 24000 sessions at a rate of 15/sec, the CPU is around 45%. When clearing all 24000 sessions and bringing them up again, the collection process suddenly is manifesting itself by generating a high CPU: it is taking up 50% of all the CPU. This issue is seen on the Cisco 10000 platform but may affect other platform also. This will likely happen all the time. This issue may cause operational impact due to high CPU utilization.

  Workaround: There is no workaround. Issue the **sh proc cpu** command to see CPU utilization.

- CSCsh74127

  Symptoms: ISIS adjacencies may not be established.

  Conditions: This symptom is observed on a Cisco 7600 series where the ISIS adjacency is configured to be established over an Ethernet Services (7600 ES20) line card with QinQ subinterfaces that are configured to support double-tagged packets when the default MTU size is 1500 bytes.

  Workaround: Configure the MTU to be 1504 bytes.

- CSCsh75457

  Symptoms: The RP may crash during the boot process of the router.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured with QoS service policies.

  Workaround: There is no workaround.

- CSCsh78416

  Symptoms: Stale routes are not flushed from the routing table after the stale path timer has expired during a graceful restart of a BGP session. As a result, all unwanted traffic continues to be processed by the router for those stale routes.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured for BGP graceful restart. The symptom occurs when, during the graceful restart of the BGP session, a non-established active session resets.

  Workaround: Clear or restart the BGP process on the router to remove all stale routes.

- CSCsh81289

  Symptoms: A Cisco 7600 series router configured for EoMPLS VCs may fail to forward disposition traffic after a router reload.

Workaround: There is no workaround.

- CSCsh85531

  Symptoms: Some E1 channels may remain down after you have reloaded a router.

  Conditions: This symptom is observed on a Cisco 7200 series that function as a PE router and that connects to a CE router. Both routers are connected through 1-port multichannel STM-1 (PA-MC-STM-1) port adapters and the **framing no-crc4** command is enabled on all interfaces of both routers.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the SONET controller of the PA-MC-STM-1 at the PE side to enable all interfaces to come up.

- CSCsh91974

  Symptoms: The Route Processor (RP) crashes.

  Conditions: Some of the Protocol Independent Multicast (PIM) CLI commands are causing the active RP to crash. The crash happens *only* when these commands are configured while in control-plane policing subconfiguration mode. Normally, any global relevant configuration should automatically exit the subconfiguration prompt and also accept the command. In this case, the PIM command is rejected and the RP crashes. The same PIM commands work fine when entered under global configuration mode (where they belong) or under other subconfiguration modes.

  Workaround: Use the **exit** command to exit the main configuration prompt before configuring PIM-related commands.

- CSCsi05069

  Symptoms: After a DCE Frame Relay subinterface is provisioned, traffic does not pass.

  Conditions: This symptom is observed on a Cisco 10000 platform when the subinterface is shut down, the configuration is applied, and then the subinterface is brought back up. This is a problem for only Frame Relay DCE; DTE and NNI work okay.

  Workaround: Configure the DLCI on the subinterface when it is not shut down.

- CSCsi14934

  Symptoms: A Traceback/CPUHOG message is observed on the active supervisor when the standby supervisor 720 is still booting up. This seems to be a transient issue that is seen at boot time.

```
*Mar 15 13:25:25.990: %SYS-SP-STDBY-3-CPUHOG: Task is running for (2000)
msecs, more than (2000)msecs (33645/33645),process = RFSS worker process.

 -Traceback= 813700C 8136E6C 8137EE0 8412870 82A4668 8A61A40 8A632A8 829C28C
8291EF0
 *Mar 15 13:25:29.271: %SYS-SP-STDBY-3-CPUHOG: Task is running for (2000)
msecs, more than (2000)msecs (33645/33645),process = RFSS worker process.
```

  Conditions: While switching from rpr to rpr-plus mode, the standby supervisor undergoes a restart, and a traceback is seen as reported by the submitter. But actually a traceback is seen at every startup not just during the mode switch. From the traceback decode, there is a double access to NVRAM through an 8-bit pointer, and this over a large NVRAM probably also causes a CPU Hog at the point of invocation of the function.

  Workaround: There is no workaround.

- CSCsi16903

  Symptoms: An IGMPv3 mode 4 group report with empty source list {} gets translated incorrectly to a mode 6 group report when using an ssm-mapped source. Expected behavior would be to translate to a mode 5 group report.

  Conditions: This symptom occurs when IGMPv3 mode 4 group report with empty source list {} is translated by static ssm-map.

  Workaround: Avoid using empty source list {} by specifying source and therefore not needing SSM static mapping.

- CSCsi17158

  Symptoms: Devices running Cisco IOS may reload with the error message “System returned to ROM by abort at PC 0x0” when processing SSHv2 sessions.

  If the vty line that is being used by SSHv2 sessions to the device is cleared while the SSH session is being processed, the next time an ssh into the device is done, the device will reload.

  Conditions: This symptom occurs when SSHv2 is deployed.

  Workaround: There are mitigations to this vulnerability: For Cisco IOS, the SSH server can be disabled by applying the command **crypto key zeroize rsa** while in configuration mode. The SSH server is enabled automatically upon generating an RSA key pair. Zeroing the RSA keys is the only way to completely disable the SSH server.

  Access to the SSH server on Cisco IOS may also be disabled via removing SSH as a valid transport protocol. This can be done by reapplying the **transport input** command with “ssh” removed from the list of permitted transports on VTY lines while in configuration mode. For example:

  ```
  line vty 0 4
  transport input telnet
  end
  ```

  If SSH server functionality is desired, access to the server can be restricted to specific source IP addresses or blocked entirely using Access Control Lists (ACLs) on the VTY lines as shown in the following URL:

  http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swacl.html#xtocid14

  More information on configuring ACLs can be found on Cisco’s public website:

  http://www.cisco.com/warp/public/707/confaccesslists.html

- CSCsi17590

  Symptoms: A CPUHOG message at the check heaps process is displayed when a large number of VRFs are configured. This may lead to BGP flapping.

  Conditions: This symptom is observed when a large number of VRFs are configured on the box.

  Workaround: Reduce the number of VRFs configured, if possible.

- CSCsi28119

  Symptoms: CPU utilization on the ES20 line cards is high with scaled EVC configurations with QoS.

  Conditions: With scaled EVC QoS configurations on ES20 line cards with traffic, CPU utilization will be normally on the higher side. Below are the observed figures. - With 8,000 EVCs configured with QoS, CPU utilization on ES20 is around 35 to 50 percent. - With 16,000 EVCs configured with QoS, CPU utilization on ES20 is around 60 to 75 percent.

  Workaround: There is no workaround.

- CSCsi32646

  Symptoms: The following message may appear on the console after a line card reset or OIR.

  ```
  %UTIL-3-IDTREE_TRACE: PW freelist DB:Duplicate ID free ...
  ```

  Conditions: This symptom is observed when xconnects are configured on the line card interfaces and multiple RP switchovers have been performed.

  Workaround: There is no workaround.

- CSCsi40467

  Symptoms: Shut down the interface. The router crashes

  Conditions: Route-map test is configured with set ip next-hop verify-availability track option. If the interface configured for track option is shutdown, then the router crashes.

  Workaround: There is no workaround.

- CSCsi41109

  Symptoms: A high CPU load occurs while prefixes are being learned or updated.

  Conditions: This symptom is observed when a large number of unique recursive paths resolve through a short-mask prefix (for example, a default route); whenever a more specific prefix is inserted, these recursive paths are re- resolved.

  Workaround: Ensure that the network has specific long-mask routes to the recursive next-hops.

- CSCsi46510

  Symptoms: After a switchover, sometimes an interface may not come up and the following message is displayed:

  ```
  PM-STDBY-4-INT_FAILUP: GigabitEthernet3/3 failed to come up. No internal VLAN
  available
  ```

  Conditions: This symptom is observed after an SSO switchover and under rare conditions.

  Workaround: There is no workaround.

- CSCsi54784

  Symptoms: A high CPU load occurs when prefixes are learned or updated.

  Conditions: This symptom is observed when a large number of unique recursive paths resolve through a short-mask prefix (for example, a default route); whenever a more specific prefix is inserted, these recursive paths are re-resolved.

  Workaround: Ensure that the network has specific long-mask routes to the recursive next hops.

- CSCsi58211

  Symptoms: Link flaps may be observed on a TenGigabitEthernet interface with XENPAK-10GB-LW under load.

  Conditions: This symptom is observed under a high-traffic test scenario of over 9 Gb traffic rate through the xenpaks.

  Workaround: The XENPAK-10GB-LW will not support over 9Gbps of traffic.

- CSCsi62313

  Symptoms: When an output QoS policy is configured on an ES20 service instance with “xconnect” or “connect” configured, the following messages will be seen:

  ```
  00:02:43: %DFCWLC_QOS-DFC4-3-EXCEEDGUARTQRATE: DFC WAN Line Card Exceeded
  Guaranteed Rates on interface - Update new queue rates: queue id 64 Cause:
  0x00060018
  ```

```
00:02:43: %DFCWLC_QOS-DFC4-3-EXCEEDGUARTQRATE: DFC WAN Line Card Exceeded
Guaranteed Rates on interface - Update new queue rates: queue id 65 Cause:
0x00060018
```

Conditions: When the total combined guaranteed rate on all service policies applied to an ES20 interface with EVCs exceeds the maximum bandwidth of the interface, the traffic on the EVCs (on which the policy is applied after the rate is exceeded) will be forwarded on a "best-effort" basis using the port's default forwarding queue.

Workaround: Do not configure output policies such that the bandwidth of the interface is oversubscribed.

- CSCsi62559

  Symptoms: OSPF packets with IP Precedence 0 are classified by SPD as priority packets. This is an error because only IP Precedence 6 packets should be classified as priority packets by SPD.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18) or a later release but may also affect other releases.

  Workaround: Use ACLs to block invalid IP control packets from reaching the control plane.

- CSCsi65922

  Symptoms: Once a BGP neighbor is configured for shutdown using "neighbor <> shutdown" Cisco IOS CLI, a subsequent "no neighbor <> shutdown" does not bring up the BGP session with its peer.

  Conditions: This symptom happens after a BGP neighbor is configured for shutdown using "neighbor <> shutdown" Cisco IOS CLI.

  Workaround: Remove the neighbor using "no neighbor <> remote-as <>" Cisco IOS CLI and then add it again.

- CSCsi68819

  Symptoms: A Cisco 10000 router may encounter a memory leak in several functions (CEF: IP ICMP Ratelimit SB, CEF: Brkr Upda, CEF: IPv4 RPF and IPv4 FIB subblock).

  Conditions: Unknown.

  Workaround: Insert a secondary PRE.

- CSCsi70224

  Symptoms: After switch-over, the standby BOOT variable might not be present when issued the **show bootvar** exec command from console port.

  Conditions: Steps to reproduce:

  1. Bootvar set in startup-config
  2. Attempt a "no boot system .." in config mode.
  3. Do a "redundancy force main-cpu" in Active and not save the configs.
  4. When the new standby comes up "bootvar" goes missing after bulk- sync.
  5. If there is another switchover, the new Active will not have the bootvar string set all and the new standby will also not have the bootvar string.

  Workaround: Make sure at least a "**boot system** ..." command exists on the running config.

- CSCsi74123

  Symptoms: A router that is running Cisco IOS Release 12.2(33)SRB2 will lose the configuration of maximum routes <value> warning-only upon reload.

Conditions: The issue is triggered by an inconsistency between the CLI and the nvgen: CLI knows about warning-only nvgen (running/startup config) knows about warn-only.

Workaround: There is no workaround. Use the command without the warning-only keyword.

Further Problem Description: In an SSO environment (with dual supervisors) this issue will stop the initial sync upon bootup and will stop the standby from booting.

The consistent correct keyword is warning-only.

- CSCsi76842

  Symptoms: The problem occurs when the encap on an interface is changed from FR to PPP/HDLC.

  Conditions: Set encap FR on an interface. Then change the encap to PPP/HDLC. It is observed that the line protocol remains down.

  Workaround: Reloading the SIP-200 module. Reloading the SPA.

- 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.

- CSCsi79155

  Symptoms: Some times on SSO switchover, the layer3 lacp channel does not come up and the following messages are seen on the standby.

  ```
  *May 7 23:17:12.333 IST: %PM-STDBY-4-INT_FAILUP: Port-channel2 failed to come up. No
  internal VLAN available
  ```

  Conditions: This is a rare occurrence and happens in a corner case.

  Workaround: Do a **shut/no shut** on the Port Channel.

- CSCsi85453

  Symptoms: The following message is seen: Config Sync: Line-by-Line sync verifying failure on command: switchport mode trunk due to parser return error

  The standby supervisor is reset.

  Conditions: This condition exists in Cisco IOS Releases 12.2SRB1 and 12.2SRB2.

  1. Trunk mode BCP is configured on a port
  2. Paste the following config for the port:

  ```
  no switchport
  switchport
  switchport mode trunk

  or paste the following config:
  no switchport
  switchport
  switchport nonegotiate

  or paste the following config:
  ```

```
no switchport
switchport
switchport trunk allowed vlan none
```

Workaround: Enter each line one at a time manually, rather than pasting multiple lines all at once.

- CSCsi86339

  Symptoms: Packets accidently go out TE FRR back up tunnel.

  Conditions: This symptom occurs when FRR is enabled on TE tunnel under some circumstances.

  Workaround: There is no workaround.

- CSCsi86691

  Symptoms: The RP processor is stacked in a process, and is not able to communicate with the SP. After a time without any notice form the SP, the RP processor decides to reload itself and SP.

  You can see the following messages in the crash information from the SP and RP:

  ```
  %Software-forced reload
  Breakpoint exception, CPU signal 23,
  ```

  And this message several times in the log information for the RP:

  ```
  %SYS-2-INTSCHED: 'idle' at level 2 -Process= "Net Input", ...
  -Traceback= ...
  ```

  Conditions: This symptom is observed under dynamic PBR configuration.

  Workaround: There is no workaround.

- CSCsi94863

  Symptoms: A Catalyst 6500 switch with WS-6704-10GE or SUP32-10GE cards using Xenpak transceivers may not enable the xenpak's transmitter upon module reload or live-insertion of the xenpak transceiver. As a result, the partner port reports that the link is down.

  Conditions: This symptom occurs when the xenpak transceiver's transmitter might not get turned on upon xenpak live-insertion, or after the module is reloaded.

  Workaround: Issuing **shut/ no shut,** will recover the interface.

  This bug is resolved in: Cisco IOS Releases 12.2(33)SRC and later, 12.2(33)SRB3 and later, 12.2(18)SXF11 and later, 12.2(33)SXH and later, CatOS 8.6(4) and later, CatOS 8.7(1) and later releases.

  Further Problem Description: A hardware race condition exists between the xenpak's TX_ON and RESET input pins. These signals are asserted each time the linecard is reloaded, and upon live-insertion of a xenpak transceiver. Variations in hardware timing within the xenpak transceiver itself sometimes causes the transceiver to incorrectly leave the transmitter disabled after exiting the reset state. This bug corrects the race condition and also insures that the driver meets the timing requirements set forth in the xenpak MSA.

- CSCsi98587

  Symptoms: MET leak is seen while running a large number of IPv4 and IPv6 mutlicast traffic.

  Conditions: The MET leak is seen only when multiple join/leave, re-routing, and few RP address/replication mode change are done.

  Workaround: There is no workaround.

- CSCsi98730

  Symptoms: The MPLS labels for packets that are forwarded via CEF and MPLS over a BGP route may not match the labels in the BGP table, which may lead to traffic loss.

  Conditions: This problem occurs under certain circumstances and timing conditions.

  Workaround: When the symptom occurs, enter the **clear ip route** command for the prefix in the VRF.

- CSCsj00870

  Symptoms: Severe IPC message leaking or BADSHARE error messages are seen during system bootup, swichtover or OIR (LC, setup):

```
c6lc2-spdbg-5-dso-b.so+0x10FAC4: verrmsg
../os/logger.c:0
c6lc2-spdbg-5-dso-b.so+0x110168: errmsg
../os/logger.c:0
c6lc2-spdbg-15-dso-b.so+0x2B7A04: datagram_done
../os/buffers.c:0
c6lc2-spdbg-16-dso-b.so+0xC2DCC:
logger_icc_callback
../const/native-sp/logger_sp.c:0
c6lc2-spdbg-13-dso-b.so+0x57BD90:
icc_request_cb
../const/native/icc_request.c:0
c6lc2-spdbg-13-dso-b.so+0x57BE10:
icc_request_cb_new
../const/native/icc_request.c:0
c6lc2-spdbg-4-dso-b.so+0xB25BC: ipc_deliver_message
../ipc/ipc_server.c:0
c6lc2-spdbg-4-dso-b.so+0xB2BA8:
ipc_process_insequence_message
../ipc/ipc_server.c:0
c6lc2-spdbg-4-dso-b.so+0xB3794: ipc_process_message
../ipc/ipc_server.c:0
c6lc2-spdbg-4-dso-b.so+0xB3DF4: ipc_process_raw_pak
../ipc/ipc_server.c:0
c6lc2-spdbg-17-dso-b.so+0x4C870:
sb1250_eobc_process_rx
../const/sb-common/sb_common_eobc.c:0
c6lc2-spdbg-17-dso-b.so+0x4D0F8:
eobc_rx_interrupt
../const/sb-common/sb_common_eobc.c:0
c6lc2-spdbg-17-dso-b.so+0x50020:
sb1250_eth_callback
../src-sibyte/dev/sb_eth.c:0
```

  Workaround: There is no workaround.

- CSCsj03212

  Symptoms: There are two vpn-spa blades configured in redundancy group. Shutting down or reloading one of the blades takes the group into bad state, and traffic does not flow through the other blade.

  Conditions: This symptom occurs when creating 1000 fvrf-ivrf-vti-eigrp tunnels, and two vpn-spa modules are configured in b2b group. Shutting down one of the SPAs or reloading it takes the group state to RECOVERY and stays there only.

  Workaround: There is no workaround but after some time when one spa comes up, other one also comes up and b2b state becomes OPERATIONAL.

- CSCsj04201

  Symptoms: The following messages are seen in the log or on the router console following a Stateful Switchover (SSO):

  ```
  %IPC-5-INVALID: Invalid dest port Dest Port 0x0 Session 0x0 Source 0x0
  %MRIB_PROXY-2-MRIB_RP_FAILED_GET_IPC:  RP failed allocating IPC buffer
                 which may lead to data loss or inconsistent MFIB states
  ```

  Conditions: This error is only seen on a router with ipv6 multicast-routing configured.

  Workaround: The problem can be cleared by toggling ipv6 multicast routing off and back on using the **[no] ipv6 multicast-routing config** command.

Note This will interrupt the forwarding of ipv6 multicast traffic.

- CSCsj09838

  Symptoms: When the BGP session between a Route Reflector (RR) and PE router flaps, the RR may no longer send some routes to the PE router.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCsi85222. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsi85222. 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 to prevent the symptom from occurring. When the symptom has occurred, enter the **clear ip bgp * all in** command on the PE router to retrieve all routes from the RR.

- CSCsj10236

  Symptoms: Multicast-intact does not work with Cisco IOS Release 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCsj14847

  Symptoms: The **crypto connect** command on a channelized T3 WAN card (serial interface in the non-channelized mode) is lost after the chassis reload or on the WAN card reload.

  Conditions: This symptom occurs with chassis reload with **crypto connect** command in the startup config for a serial interface. Reload of the WAN card with the **crypro connect** command configured on the serial interface.

  Workaround: Reconfigure the **crypto connect** command.

- CSCsj32013

  Symptoms: A Cisco 12000 series router may crash unexpectedly.

Conditions: This symptom occurs only on Cisco IOS Release 12.0(32)SY0f.

Workaround: There is no workaround.

- 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.

- CSCsj36620

  Symptoms: The router crashes because of heartbeat failure between RP and SP. The RP is spending 99% at the interrupt level trying to process MPLS packets that have been punted to the RP from EARL because the adjacency entry for tag2tag is dropped right after the core facing line card is reloaded.

  Conditions: This symptom occurs after OIR the ES-20 line card.

  Workaround: There is no workaround.

  Further Problem Description: MPLS packets should never be processed when the incoming interface has xconnect, and MPLS is not enabled on the interface, which happens to be the case here.

  The fix is to drop the packet in IBC code if the packet is an MPLS packet, and MPLS is not enabled on the interface.

- CSCsj40695

  Symptoms: A Cisco router may become unresponsive or reload unexpectedly when an Embedded Event Manager (EEM) Tool Command Language (Tcl) policy that has an invalid policy registration line is registered.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image later than Release 12.4(11)T when the policy registration line is malformed. This line may become malformed when the Tcl policy is saved with a program that inserts new lines at locations where you do not expect them.

  Workaround: Before the policy is registered, inspect the policy by entering the **more flashdevice:filename.tcl** command to ensure that the script does not have a malformed event registration line.

- CSCsj47433

  Symptoms: On Cisco 7600 routers with a SIP-400 line card, packets with more than 1492 bytes may be dropped on the EoMPLS imposition path.

  Conditions: This issue is seen on routers that are running Cisco IOS Release 12.2(33)SRB2. The issue is fixed in Cisco IOS Releases 12.2(33)SRB3 and 12.2(33)SRC. Ingress EoMPLS packets to the SIP-400 that are greater than 1492 bytes (but less than the 1500 byte MTU) may erroneously be dropped on the line card. The size of the imposition labels is incorrectly included in the MTU calculation causing the drops to occur in this situation.

  Workaround: There is no workaround.

- CSCsj48440

  Symptoms: Packets “returned” from a WCCP appliance (web-cache) for further forwarding are always processed by the RP leading to elevated CPU usage.

  Conditions: This symptom is observed on a Cisco 7600 series router for WCCP redirection and with “L2 return” being used to return traffic from the appliance to the router. Further the router must either be configured for outbound redirection (**ip wccp** <*service*> redirect out) or the appliance must have selected hash assignment.

  Workaround: If the appliance is resident on its own subnet, apply the WCCP command **ip wccp redirect exclude in** to the appliance facing interface. Alternately use mask assignment and input redirection (**ip wccp** <*service*> redirect in).

- CSCsj49216

  Symptoms: The eBGP session for IPv4 does not come up.

  Conditions: This symptom occurs when address family IPv4 is removed from VPN configuration. All corresponding eBGP configurations are automatically removed. The problem happens after everything is added back.

  Workaround: There is no workaround.

- CSCsj53663

  Symptoms: A Cisco platform may reload when you configure or unconfigure an EEM policy.

  Conditions: This symptom is observed only on a Cisco platform that runs a modular Cisco IOS software image when a syslog message is being generated while you configure or unconfigure the EEM policy.

  Workaround: Do not configure or unconfigure an EEM policy while a syslog message is being generated.

- CSCsj56281

  Symptoms: Inherit peer-policy does not work after router reloads.

  Workaround: There is no workaround.

- CSCsj64154

  Symptoms: After reloading a Cisco 7600 router that is running Cisco IOS Release 12.2(33)SRB1, the following error message is displayed:

  ```
  %SIP200_MP-4-PAUSE: Non-master CPU is suspended for too long, from 0x4022F650(2) to
  0x4022F6A0 for 329873 CPU cycles. -Traceback= <different tracebacks>
  ```

  Message are logged continuously.

  Conditions: This symptom is observed on a Cisco 7600, SIP-200.

  Workaround: There is no workaround, but there is no impact on user traffic.

- CSCsj65189

  Symptoms: Traffic stops over EOM ckt after SSO and followed by TE FRR cutover.

  Conditions: The issue seen here is that after the SSO switchover at cat5 the local EOM label at cat5 gets changed and the same gets updated at cat2 for the corresponding VC correctly. Now, when the FRR cutover is performed at cat5, the local VC label gets changed for the second time and the same also gets updated at cat2 for the corresponding ckts. However the label push gets messed up at cat2, which results in EOM traffic loss from cat2 to cat5 but the other direction traffic passes fine. If the same FRR cutover is performed before the SSO switchover at cat5 then there will not be any problem. It is only after the SSO when this issue is observed. Please refer the enclosure BigDescription for more details.

Workaround: There is no workaround.

- CSCsj67096

  Symptoms: On a Cisco Catalyst 6500 series switch Sup720 that is running Cisco IOS Release 12.2(18)SXF7, if there is a port-channel with combination of non-fabric enabled and fabric enabled card (here WS-X6408 and WS-X6516) and this port-channel is configured as a trunk.

  The traffic comes on port-channel trunk on one VLAN, gets source NATed on Sup720 and sent back on same port-channel on another VLAN.

  The traffic gets dropped for the stream coming on one port of the channel in a VLAN and sent back on 2nd port on another VLAN. The issue is that the source index is not getting re-written after NAT, so the traffic gets dropped.

  Note that if the traffic comes on one port of the channel and goes back on the same port, the packets get rewritten correctly. Partial packet loss.

  Conditions: This issue happens only with Sup720 that is running Cisco IOS with port-channel member ports on WS-X6408 and WS-X6516 line cards.

  Workaround: Shut one member of the port-channel, so that traffic comes one a port, gets NATed/routed and goes back on the same port on the switch. Or Use either fabric-enabled cards or non-fabric enabled card in the port-channel. DO NOT USE combination of non-fabric enabled and fabric enabled cards.

- CSCsj68911

  Symptoms: On a Cisco Catalyst 6500 system that is running Cisco IOS Release 12.2(18)SXF9 and DFC enabled line cards, approximately 90K memory will be held on each DFC when a redundancy force-switchover is issued. The memory is never released afterwards. This will happen each time a redundancy force-switchover (both RPR+ and SSO) is issued.

  Conditions: This symptom only affects line cards with DFC daughterboards.

  Workaround: There is no workaround.

- CSCsj70109

  Symptoms: A 100% traffic loss is observed from hub to all the spoke devices.

  Conditions: This symptom occurs when hub and spoke topology with IPSEC when RRI (Reverse Route Injection) is configured on spokes and hub device the static routes to the spokes are not injected in the routing table of the hub.

  Workaround: Manually configure the static routes on the hub router.

- 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.

- CSCsj74617

  Symptoms: Only the last entry of “mpls static” and “moi” CLIs that are configured on active RP can get synced to slave RP.

  Conditions: This issue is found on Cisco 7600 platform under SSO HA status.

  Workaround: There is no workaround.

- 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
```

- CSCsj83966

  Symptoms: The message CPU HOG will appear in the screen.

  Conditions: This symptom occurs when a lot of interfaces are coming up/down at the same time. The syslog used to process 100 traps at one time, which causes CPU HOG

  Workaround: The condition will not appear if there are comparatively less number of interfaces. Also, unconfigure the trap from **sh run** will prevent from this issue.

- 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.

- CSCsj88017

  Symptoms: A sip400 line card on a Cisco 7600 has a large number (~8K) of EVCs configured on its interfaces. QoS service-policies are applied to all of the EVCs. When the line card is reloaded, only a subset of the configured EVCs come back up.

Conditions: The issue is only seen when QoS service-policies are applied to a scaled EVC configuration. The problem is limited to distributed platforms like the Cisco 7600.

Workaround: Reapply missing EVC configurations when the line card comes up.

Further Problem Description: The failure of some EVCs to come up is due to contention for resources between the interface and QoS modules. The fix balances CPU usage among the modules to prevent timeouts and other error conditions.

- CSCsj89544

  Symptoms: If a BGP keepalive message fails to be sent to a BGP peer because the transport link is down, the neighbor BGP peer does not accept any further keepalive packets even though TCP retransmits the failed message using a backup path. This eventually causes the BGP peer to go down because of holdtime expiration.

  Conditions: This happens when TCP retransmissions occur on MPLS-enabled network. This is seen only when MPLS is configured on Catalyst 6500 or Cisco 7600.

  Workaround: There is no workaround.

- CSCsj89931

  Symptoms: Issue copy file running-config results in Line-by-Line sync PRC error with cfg consists of CLI that trigger parser inexplicit exit, e.g controller T1 9/0/0.

  Workaround: There is no workaround.

- CSCsj90039

  Symptoms: All traffic that needs to be processed by input on the SVI is dropped.

  Conditions: Input queue wedge at the SVI.

  Workaround: Reload router.

- CSCsj91123

  Symptoms: Double freeing of freed memory. Router reloads after authentication attempt fails on vty/console.

  Conditions: While performing AAA accounting, the accounting structure was freed twice, which results in crash. The below CLI is configured **aaa accounting send stop-record authentication failure**, which sends a stop record for authentication failure.

  Workaround: Remove **aaa accounting send stop-record authentication failure**, which will disable sending of the stop record at authentication failure.

- CSCsj97484

  Symptoms: The router may crash when the line card is booted.

  Conditions: This problem is not easily reproducible. The problem may be experienced if there are heavy distribution traffic to the line cards.

  Workaround: There is no workaround.

- CSCsj99354

  Symptoms: If an interface does not have IP address or IPv6 addresses, the **passive-interface** command will not be shown under “router ospf ...”.

  Conditions: This symptom is seen when running Cisco IOS Release 12.0S images or images from Cisco IOS Release 12.2SR.

  Workaround: Configure either IP or IPv6 address for the interface.

- CSCsk02962

  Symptoms: When Egress Multicast replication mode is used on a Cisco 6500 platform with PFC3x, after the SSO switchover occurs, the new active supervisor SP may reload on MET reconstruction.

  Conditions: This symptom is observed with Multicast Egress Replication and SSO redundancy mode.

  Workaround: Do not use SSO HA in conjunction with Egress Multicast Replication Mode.

- CSCsk04287

  Symptoms: Switch crashes due to EIGRP.

  Messages found: Debug Exception (Could be NULL pointer dereference) Exception (0x2000)!

  Conditions: This is seen on a Cisco 3560 router that is running Cisco IOS Release 12.2(40)SE.

  Workaround: There is no workaround.

- 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.

  Workarounds:

  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.

- CSCsk07418

  Symptoms: If one interface has different passive interface configurations than other interface, parser return code will be inconsistent between HA routers, and standby router will reload.

  Conditions: Set passive interface configuration under “router isis” or “router ospf”. Set one interface with different passive interface configuration. Repeat these two config CLIs several times and then standby router will reload.

  Workaround: Do not set an interface with different passive interface configuration in HA SSO mode.

- CSCsk08681

  Symptoms: On physical OIR removal followed by insert of line card into chassis, FIB errors may be seen on the Standby SUP console.

  Conditions: This symptom will only happen if “module clear-config” is present in the configuration.

  Workaround: Remove “module clear-config” from the configuration.

  Further Problem Description: This command is not supported by ES20 or SIP-600 line cards.

- CSCsk10895

  Symptoms: After an SSO, LDP and BGP sessions might flap.

  Conditions: This symptom happens only if the **mpls ldp explicit- null** command is enabled.

  Workaround: Disable explicit-null for LDP.

  Further Problem Description: This happens because MPLS MFI deletes the explicit-null label. This behavior will be fixed by another DDTS CSCsk28546.

  This DDTS fix is to avoid freeing the global table reserved VLAN as long as MPLS is enabled in the box.

- CSCsk15606

  Symptoms: Stored configurations in the CMTS (stored in disk or in bootflash), when copied to the running configuration, the secondary PRE reloads.

  Conditions: This symptom occurs when the stored configurations in the CMTS (disk or bootlfash) are copied to the running configuration.

  Workaround: Remove the CLIs “auto-sync standard” and “no file verify auto” from the stored configuration.

- CSCsk16937

  Symptoms: A memory leak at atm_add_aal5_layer is observed.

  Conditions: This symptom occurs when testing of ATM with a large number of subinterfaces configured.

  Workaround: There is no workaround.

- 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.

- CSCsk18206

  Symptoms: TCAM programming problem is encountered when PBR and NAT are involved.

  Conditions: TCAM does not always get programmed properly when Policy Based Routing and NAT are present in the configuration.

  Workaround: To restore service, follow these steps to force a TCAM adj recalculation:

  Step 1: Remove PBR service policy from all VLAN interfaces which have PBR. Then reapply PBR policy on those impacted VLAN interfaces.

  Step 1 is the preferred method to force a TCAM adj recalculation without triggering routing updates to the rest of the network. If the issue persists, then proceed to step 2.

  Step 2: Shut/unshut the impacted VLAN interface and other VLAN interfaces that share the same PBR policy with the impacted interface.

  Further Problem Description: Troubleshooting details: Follow these steps to identify a reoccurrence of the TCAM adj issue and identify the interfaces that are experiencing traffic interruption.

Step 1: Check what indexes are used in TCAM adj.

Step 2: Check the REDIRECT adjacency indexes in tcam interface for potentially affected VLANs and make sure it only has indexes which are listed in the TCAM adj output. You will have to check this for all interfaces configured with PBR.

```
sp#sh tcam int vlan <affected_VLAN> acl in ip de | inc indx:
```

- CSCsk19817

  Symptoms: The error message “pm failed get pm mp semaphore” is seen on the **shut/no shut** of an interface.

  Conditions: This message can be seen on any interface under stress if any line card in the system is under stress and takes more time to process commands from supervisor.

  Workaround: There is no workaround.

  Further Problem Description: Apart from the error message, **shut/no shut** takes two minutes, and the consoles freezes during this time.

- CSCsk21737

  Symptoms: Ports connected to newly installed ES20 line card will be up, while ES20 port shows admin down.

  Conditions: Ports connected to newly installed ES20 line card will be up, while ES20 port shows admin down.

  Workaround: Do not connect the fiber until ready to use.

- CSCsk24272

  Symptoms: RP crashes due to memory leak in I/O big buffers.

  Conditions: This symptom is observed when flow export is configured with 127.0.0.x address

  Workaround: Remove flow export configuration with 127.0.0.x address.

- CSCsk28546

  Symptoms: In a setup with 32k EVCs configured, when the standby is reloading mpls reserved labels are deleted in the active. Explicit-null getting deleted was affecting the 7600 platform because of the way recirculation is handled.

  Conditions: The problem is triggered from active RP when standby is coming UP.

  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.

- CSCsk33724

  Symptoms: Starting release 12.2(33)SXH, DOM feature will not be supported on some transceiver types. The list of supported transceiver types can be obtained from a running switch using the command “show interface transceiver supported-list”. This change has been made to handle cases where the DOM thresholds or operating values are inaccurate thereby resulting in bogus SNMP trap notifications.

Conditions: This issue is seen only with the following conditions:

1. 12.2(33)SXH software and later only.
2. Transceivers listed as “unsupported” in output of **show interface transceiver supported-list** command.

Workaround: There is no workaround.

- CSCsk33740

  Symptoms: Increasing the IPSec anti-replay window size to extended replay window size (128-1024) by using 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** [<*extended replay window size*] and then reset the VPN SPA.

- CSCsk33832

  Symptoms: Traffic forwarding will be affected.

  Conditions: This symptom is observed after resting the hw module, and the traffic in the E-gress (Imposition path) direction did not recover fully after the line card came up. In another instance all imposition traffic failed after card reset.

  Workaround: A “clear ip ospf process” clears the problem.

- CSCsk34237

  Symptoms: Egress multicast replication stops working due to WCCP.

  Conditions: This symptom is observed when WCCP feature is present, and Egress multicast replication mode is configured on Cisco Catalyst 6500 switches.

  Trigger: When the WCCP service goes down.

  Frequency: Always.

  Root cause: Wrong service adjacency being updated when WCCP goes down.

  Impact: This will impact Multicast Traffic Forwarding and egress multicast replication will not work.

  Workaround: Switch to ingress multicast replication mode using the **mls ip multicast replication-mode ingress** command.

  Issue Verification: The hardware programming shown via **sh mls ip multicast group** *group-address* and **show mls cef ip multicast source** *source-address* **group** *group-address* **det** looks correct, and the traffic counters for each is incrementing but a sniffer trace and the interface statistics taken on the downstream switch show no multicast data received.

- CSCsk38937

  Symptoms: Loss of traffic for more than 15 seconds after second cutover.

  Conditions: This symptom occurs after performing two cutovers.

  Workaround: There is no workaround. Traffic recovers after 15 seconds.

- CSCsk39484

  Symptoms: A %CBUS-3-CCBPTIMEOUT message is generation as part of an on-line insertion and removal operation.

  Conditions: The message will generally be seen with OIRs for specialized equipment such as an IMA controller.

  Workaround: There is no workaround. There is no operational impact.

  Further Problem Description: The message arises from an attempt to synchronize some interface state information (specifically, the rate-interval). Synchronization is sometimes attempted when it is not possible to deliver a message. In all such cases, there is actually no need to do the synchronization so there is no impact to the router.

- 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)
  ```

- CSCsk41142

  Symptoms: When 32k xconnect configs are copied to running config, RP and SP crash.

  Conditions: This symptom is observed on a system that has two `20X1` and one `2X10GE`. The configuration has both ingress policing and egress shaping on all 32k EVCs.

  Workaround: There is no workaround.

- CSCsk42983

  Symptoms: The following traceback is seen on 7600 router.

  ```
  On 1:Sep 6 07:59:47.879 PST: %C6K_PROCMIB-DFC1-3-IPC_TRANSMIT_FAIL: Failed to send
  process statistics update : error code = re-init
  -Traceback= 2042B85C 2042BDA0 20CA9C08 20CA9C78 20CA9E28 20CA9F30
  ```

Conditions: Stressful IPC conditions causing IPC messages to be dropped.

Workaround: There is no workaround.

- CSCsk43673

  Symptoms: Network RF client might take more time to complete RF_PROG_ACTIVE progression during switchover.

  Conditions: When more than thousand interfaces are configured on a router.

  Workaround: There is no workaround.

- CSCsk44233

  Symptoms: There is possible memory corruption during routemap deletion.

  Conditions: This symptom occurs when BGP is running.

  Workaround: There is no workaround.

- CSCsk46560

  Symptoms: On reload of chassis or SPA, copper ports do not come up when issuing **no shut**.

  Conditions: Can occur with copper SFP ports on SIP-400, SIP-600 and ES20 20x1GE.

  Workaround: Reload line card or SPA after port configuration is **no shut**.

- CSCsk47888

  Symptoms: The standby processor continuously reloads due to the failure of bulk sync.

  Conditions: The IP address of the interface is configured with the same IP address as the HSRP virtual IP address. This is can be performed whilst the interface is in the shutdown state.

  Workaround: The user must avoid sharing the interface IP address with the HSRP virtual IP.

- CSCsk48182

  Symptoms: A router will crash with SSO with the configurations attached in the **show run** command output.

  Conditions: This symptom occurs with SSO.

  Workaround: There is no workaround.

- CSCsk48940

  Symptoms: “Class-Default” counters are not accounted and missed in the show policy-map o/p.

  Conditions: When SIP600 or ES20 are used as an MPLS/core facing interface for PXF based EoMPLS or VPLS, class-default counters are not updated.

  Workaround: There is no workaround.

  Further Problem Description: “Class-Default” counters are not getting updated in “show policy-map interface <>” output when we have a QOS policy attached to the interface.

- CSCsk49638

  Symptoms: The primary tail-end segment of the LS connection backed up PW remains inactive even after **no-shut** has been done.

  Conditions: **Shut/no-shut** should have been done on the primary tail-end.

  Workaround: There is no workaround.

- CSCsk51160

  Symptoms: When hierarchical QOS is configured and no queuing action is specified for a class, matching for that class fails to work.

Conditions: This symptom is only applicable when the class has no queuing actions specified.

Workaround: Add a queuing action to the class.

- CSCsk54938

  Symptoms: Packets with a source mac address beginning with 0xA100 may be dropped by SIP600 for VPLS and SVI based EOMPLS imposition.

  Conditions: If CE originating traffic is originated with 0xA100 in the first two bytes of the source mac address the MPLS core facing SIP600 may drop the imposition traffic.

  Workaround: 0xA100 is not a realistic mac address seen in real world configurations and as such does not pose an immediate risk.

- CSCsk55423

  Symptoms: This bug manifests itself as BGP packets ending up in the high priority extended headroom (as per SPD). The fix makes sure that such packets are placed in just the plain headroom and not the extended headroom.

- CSCsk55892

  Symptoms: OSPF-3-DBEXIST messages can be seen in the log.

  Additionally OSPF neighbor may flap due too many retransmissions. In some cases the flapping may be permanent and occurs during refresh of the affected LSA (period 30 minutes).

  Conditions: This symptom is observed on a router that is running Cisco IOS Release 12.2(33)SRB image. Other Cisco IOS versions are not affected. Router is an NSSA ABR. ABR originates two external type-5 LSAs which have conflicting link-state ID.

  Workaround: Clear ip ospf process may clear OSPF dbase which may stop flapping.

  More details: An example of the problematic environment: Under ospf router it is configured "redistribute static". Route to null is configured, for example ip route 10.0.0.0 255.255.0.0 null0. Type-5 LSA has LSA ID 10.0.0.0. There is the same route but with longer mask originated by ASBR in the NSS Area (type-7 external), for example 10.0.0.0 255.255.255.0. This route is translated to external type-5 LSA, and under normal circumstances should have also LSA ID 10.0.0.0. However so as not to conflict if LSA ID 10.0.0.0 already exists, this LSA should be originated with host bits set, it means LSA ID is 10.0.0.255.

  These problems have been experienced if conflicting type-5 LSAs should be originated:

  - Type-5 LSA with shorter mask is not originated from type-7 LSA, error message OSPF-3-DBEXIST is printed.
  - If two type-5 LSAs from above example are originated (10.0.0.0 /16 and 10.0.0.255 /24) and 10.0.0.255 /24 should be flushed because the route is not available any more, ABR by mistake flushes LSA ID 10.0.0.0 which leads into unpredictable behavior and usually into neighbor flap.

- CSCsk56788

  Symptoms: High CPU usage observed due to the "BGP Router" process when there are BGP remote neighbors that are not active. The problem happens when a couple of BGP neighbors are activated on the router and not configured on the peer router. Theoretically, It could also happen if for some reason some sessions just keep trying to get established but keep failing.

  Conditions: This symptom occurs when there are inactive BGP neighbors.

  Trigger: BGP trying to establish a TCP session but not getting an "Ack" from the other end.

  Root Cause: This problem happens because BGP is busy trying to open an Active connection which fails since the peer does not have the corresponding neighbor configured for that Address Family. When we go through the heavy-duty reset processing, it leads to the high CPU usage.

Impact: High CPU usage.

Workaround: One of the following is a workaround to this issue:

- Removing the neighbors which are configured only on one peer and not on the other peer.
- Putting the neighbor in shutdown mode in BGP config via the command neighbor x.x.x.x shutdown.
- -Putting the neighbor in passive mode via the command neighbor x.x.x.x transport connection-mode passive.

- CSCsk59515

  Symptoms: The BGP session will be reset during the **no neighbor max-prefix** command (with single session).

  Conditions: This symptom occurs when the BGP session will be reset unnecessarily during the **no neighbor max-prefix** command (with single session configuration). The issue is not observed with BGP multi-session.

  Workaround: There is no workaround.

- CSCsk60112

  Symptoms: Uninitialized memory causes failures when LSP ping is performed.

  Conditions: This error occurs when the allocated memory is non-zero.

  Workaround: There is no workaround.

- 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.

- CSCsk60912

  Symptoms: MPLS forwarding table is empty on standby RP.

  Conditions: This symptom is seen after ISSU loadversion, or simply when standby RP is reloaded.

  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.

- CSCsk62514

  When applying large number (over thousands) of VRF configuration with BGP enabled to a router, you may observe that it takes longer time to complete the configuration. For example, when copying a large VRF configuration file into the running-config of a router, it will take longer time to transfer the configuration data.

  There is no work around.

- 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 configs
  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.

- CSCsk64223

  Symptoms: When “no router bgp xx” is configured, the following error message may be seen and the router may crash:

  ```
  %IPRT-3-BAD_PDB_HANDLE: Pdb handle error 1040000, 0000, 0, 00000000, 76E60000, 00
  -Process= "IP RIB

  Update", ipl= 0, pid= 248

  -Traceback= 4062C0A0 40CB7E08 40CD10D8 40CD1924
  ```

  Conditions: This symptom is seen when BGP is enabled on a large number of VRFs and has a significant number of routes in each VRF.

  Workaround: There is no workaround.

- CSCsk64358

  Symptoms: MIB fields related to high capacity error counters may be incorrect.

  Conditions: If customer tracks high capacity error counters, they will be impacted.

  Workaround: There is no workaround.

- CSCsk64625

  Symptoms: Core facing traffic may be dropped for vpls/eompls when using sip600/es20 as mpls core facing interface.

  Conditions: When a sip600/es20 interface is included as an explicit path in a tunnel with multiple path options, traffic may be dropped when the path switches from one local interface to another, or when traffic switches from a non-local interface to a local interface when the egress path for the tunnel is changed.

  Workaround: There is no workaround.

- CSCsk65338

  Symptoms: Line protocol and DLCIs flap on MFR interfaces after SSO switchover on a Cisco 7600 platform.

  Conditions: The flap may occur for MFR interfaces which are LMI DTE and which do not have an explicit LMI type configured.

  Workaround: Configure an explicit LMI type on MFR DTE interface rather than using autosense.

- CSCsk65860

  Symptoms: Security ACLs along with “ip unicast verify” CLI break Client traffic to real servers.

  Conditions: Interface VLAN55 IP address 10.10.10.187 255.255.255.0 ip access-group 120 in ip access-group 121 out ip verify unicast source reachable-via rx allow-self-ping end.

  The above CLIs are configured on the interface/VLAN to which the real Servers are connected.

  Workaround: There is no workaround.

- CSCsk67417

  Symptoms: Router crashes when two or more users display Dynamic ARP Inspection log table at the same time with the **show ip arp inspection log** command.

  Conditions: This symptom occurs when DAI is configured and new ARP requests are coming on the DAI configured interface.

  Workaround: Do not display DAI logs simultaneously with the **show ip arp inspection log** command.

- CSCsk68846

  Symptoms: Router crashes when removing grand child policy.

  Conditions: This symptom is seen in Cisco 7304 router.

  Workaround: There is no workaround.

- CSCsk69408

  Symptoms: On doing line card reset on simple MLP bundles with traffic flowing, some of the multilink bundles drop the packets and do not recover after all the bundles come up.

  Conditions: This symptom happens on a Cisco 7600 router on a simple MLP bundle with service policy attached. Class voice is defined and given 50 percent priority. It specifically occurs when links are added from different SPAs and traffic is flowing.

  Workaround: Remove the service policy and reattach it.

- CSCsk70087

  Symptoms: The RP crashinfo reports the following:

  ```
  %C6K_PLATFORM-2-PEER_RESET: RP is being reset by the SP
  %Software-forced reload


  Breakpoint exception, CPU signal 23, PC = 0x41CDA8E4
  ```

  Since the crash is triggered by the SP, the crashinfo in sup-bootflash logged the following:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address
   addr=0x0, pc=0x40362F24, ra=0x40363000, sp=0x43A179F8
  %ALIGN-1-FATAL: Illegal access to a low address
   addr=0x0, pc=0x40362F24, ra=0x40363000, sp=0x43A179F8
  ```

```
TLB (store) exception, CPU signal 10, PC = 0x40362F24
```

Conditions: This problem is seen at a customer site. Hardware and software version info is as follows: WS-SUP720-3B running Cisco IOS Release 12.2(18)SXF2. The trigger for the crash is unknown.

Workaround: There is no workaround.

If you are a customer running into this, please collect the following information and contact Cisco/TAC: sh tech crashinfo from sup-bootflash (for SP) and bootflash (for RP) log entries taken from the syslog server for 1 week period leading to the crash.

In the case notes, please include the following:

1. Hardware changes done in the recent past
2. Network events that occurred at the time of the crash
3. List of Management applications polling this device

- CSCsk70247

  Symptoms: %INTR_MGR-DFC3-3-BURST: Parsing Engine(X-Chip) [0]:Inbound Parser

  Conditions: This symptom is seen during large SwEoMPLS configuration. It does not happen all the time.

  Workaround: There is no workaround.

  Further Problem Description: These errors occur for malformed mac notification packet sent from one line card to a sip-600 or es20g line card. An interrupt is logged because of problems with the IPv4 part of the data, but the mac information is still recorded. Packets are not lost with this error.

- CSCsk72417

  Symptoms: Crash is seen resetting cheronia or samboni.

  Conditions: This symptom happens only to the RSP platforms, as tftpboot path is missing.

  Workaround: There is no workaround.

- 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

- 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.

- 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 serial ATM 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.

- CSCsk80552

  Symptoms: Delay seen in forming of PIM Auto RP mapping. Whenever a link flaps, the graft messages are sent for faster convergence and since these get dropped over the MDT tunnel, there is a delay in convergence.

  Conditions: On networks with mVPN deployment and PIM-DM in the core, an interface flap on the PE/CE router may cause delay in forming PIM auto-rp mapping.

  The issue causes traffic black holing and affects the sources and receivers in the network, if the following conditions hold TRUE a. Network has MPVN deployment, and the path between source and receiver has to traverse through the MPVN cloud b. The issue is specific to 6500 and 7600 series routers, so there should be at least one 6500 or a 7600 decapsulating router (PE) present in the MPVN deployment, along the path between source and the receiver

  Workaround: To migrate to PIM-SM. No functionality is affected and the fix for the same is available in SXI release through the commit of CSCsk80552

  Further Problem Description: The PIM-DM graft messages, unlike other PIM-DM control packets are unicast packets. These packets when sent over the MDT tunnel, are encapped with multicast MAC address and an unicast IP address (Destination IP of the Tunnel), such packets are not replicated and are dropped.

- CSCsk80934

  Symptoms: When a line card has a power convertor failure, the line card will get power cycle without proper error message to indicate the failure.

  Conditions: This symptom is caused by a hardware power convertor failure.

  Workaround: This problem has been fixed, if the software detects the line card power convertor, and it will print/generate a syslog message to indicate the failure.

- CSCsk82821

  Symptoms: The UUT is not able to receive the large ICMP message.

  Conditions: This symptom occurs on the s72033-adventerprisek9_wan_dbg-vz.122-32.8.11.SX117 image.

  Workaround: There is no workaround.

- CSCsk83524

  Symptoms: L3 physical interface “input drop” counter in **show interface** *x/y* output is incrementing at the same pace as “overrun” counter. The definition of these two counters is completely different.

  Conditions: In nutshell, “input drop” counter represents packets dropped by RP in software when input queue is full and RP throttles the interface. Overrun counter represents packets dropped in hardware due to lack of rx buffers in port asic.

  At the moment, L3 physical interface “input drop” counter counts both software and hardware dropped packets, which is incorrect.

  Workaround: There is no workaround.

  Further Problem Description: Current PM counters handling code does not distinguish L2 Switchports from L3 Routed Ports. For each port on the system PM will collect stats and counters from the line card and store them in both port_data counter structure and also roll them up to IDB counters.

Since the definition of “input drop” is specific for L3 Routed Interfaces and should be incremented only when the software process switching runs out the capacity to enqueue and process incoming packets. For packets drops at the hardware or firmware level due to overrunning of hardware queue (ifInDiscards) is kept in a counter in the PM and not be displayed as part of “input drops”.

- CSCsk85987

  Symptoms: The line protocol state of SVI interfaces is incorrectly marked “down” after an SSO switchover.

  Conditions: This symptom is sometimes seen on the second and subsequent SSO switchovers.

  Workaround: Reload the line card that has the affected interface.

- 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.

- CSCsk87523

  Symptoms: State of the AAA server always shows UP, even when the interface connected to server was shutdown (cnx port is shut (admin down)).

  Conditions: This symptom occurs when configuring the following CLI on NAS:

  ```
  "radius-server host <ip add> auth-port 2295 acct-port 2296 test username sdanda
  idle-time 1 key cisco"
  ```

  With this CLI configured, NAS requests are sent to server and then disconnecting the interface connected to AAA server from NAS and when issuing the **sh aaa servers** command shows the state of the AAA server as UP/DOWN. The impact is a display issue.

  Workaround: There is no workaround.

- CSCsk88656

  Symptoms: Link-flap is observed on OSM-2+4GE-WAN+ after reload.

  Conditions:

  - Link-flap is observed on SXF-train by “reload” or “hw module <mod> reset”.
  - The symptom is observed on SXF-train with SUP2 or SUP720.
  - Not observed on Cisco IOS Releases 12.1(27b)E3 and 12.1(26)E1 with SUP2.

  Workaround: There is no workaround.

- CSCsk89335

  Symptoms: Observed power supply PWR-6000-DC mismatch.

  Conditions: This error occurs after Supervisor SSO switchover. The chassis is equipped with dual PWR-6000-DC power supplies. Both have the same input power. This is a false alarm.

  Workaround: There is no workaround.

- CSCsk93366

  Symptoms: The crash has been observed “once” on an RSP720 along with error messages.

  Conditions: The crash happens when an ESM20 card is reset. AToM must be involved to expose the problem.

Workaround: There is no workaround.

Further Problem Description: This is not specific to ESM20 card, and it is a platform independent issue. It is not a corner case and FIX required for all AToM supporting images.

- CSCsk99465

  Symptoms: A Cisco 7600 router that is configured with MPB in a SSO HA configuration may display a message as follows:

  ```
  %ISSU-3-NOT_FIND_MSG_SES: Cannot find message session(0) to get msg mtu
  ```

  Conditions: This behavior exists for MPB in SR releases since SRC. The problem is seen when the Standby Supervisor and the line card on which MPB is configured get reset. After this, if the line card comes back online before the ISSU negotiation between the Active Supervisor and the Standby Supervisor is completed, this error message will be seen.

  Workaround: Avoid a double-fault situation as above in which the Standby supervisor and the line card get reset at the same time.

- CSCsk99687

  Symptoms: It is very rare to hit this bug. When hit the router is going to crash.

  Conditions: This symptom is seen during the ISSU runversion.

  Workaround: There is no workaround.

- CSCsk99739

  Symptoms: A Cisco 7600 L2WAN system crash is observed.

  Conditions: This symptom occurs due to the internal test beds and is observed after the routers are booted up and reproducible.

  Workaround: There is no workaround.

- CSCsl00041

  Symptoms: The **show policy-map** counts do not include EoMPLS/VPLS packet counts on ES20/SIP600 MPLS core facing interfaces.

  Conditions: If an output policy is configured on a SIP600/ES20 mpls facing interface, the **show policy-map** counts will not include the EoMPLS/VPLS traffic if all 8 EXP values are matched in nondefault classes. This does not affect pure MPLS label switched traffic, only output policy counters that would increment due to EoMPLS/VPLS imposition. Below is an example configuration that will trigger the issue:

  ```
  ## all 8 exp's configured in classes matched in policy
  class-map match-any EXP7
    match mpls experimental topmost 7
  class-map match-any EXP6
    match mpls experimental topmost 6
  class-map match-any EXP5-4
    match mpls experimental topmost 5
    match mpls experimental topmost 4
  class-map match-any EXP3-2
    match mpls experimental topmost 3
    match mpls experimental topmost 2
  class-map match-any EXP1-0
    match mpls experimental topmost 1
    match mpls experimental topmost 0
  ```

```
policy-map WFQ
  class EXP7
    bandwidth 100000
 class EXP6
    bandwidth 10000
  class EXP5-4
    bandwidth 100000
  class EXP3-2
    bandwidth 100000
  class EXP1-0
    bandwidth 200000
  class class-default

interface GigabitEthernet2/0/0
 ip address 10.1.1.1 255.255.255.252
 no mls qos trust
 mpls traffic-eng tunnels
 mpls label protocol ldp
 mpls ip
 service-policy output WFQ
```

Workaround: Configure the policy such that at least one EXP value goes to the class-default.

- CSCsl00221

  Symptoms: There is memory corruption with malloc_lite.

  Conditions: This symptom is seen sometimes on boxes using malloc_lite feature, i.e, with **memory lite** configured on the box.

  Workaround: Disable malloc_lite using **no memory lite** configuration command.

- CSCsl04908

  Symptoms: A Cisco 6500 or 7600 router that is running WCCP may reload when an interface is shutdown.

  Conditions: The router must be configured for WCCP L2 redirection with mask assignment and input redirection on one or more interfaces. The reload is triggered when the appliance facing interface is shutdown.

  Workaround: If possible, shutdown WCCP on the appliance before shutting down the router interface. Alternatively remove the WCCP configuration before shutting down the interface.

  Further Problem Description: The issue only occurs for Cisco 7600 and Cisco 6500. The code commits to other trains are for code consistency reasons only.

  When the system reloads the resultant error looks similar to the following:

```
Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x41A4686C


-Traceback= 41A4686C 419750CC 41968AD0 41969328 4196911C 419692F4 41996D74 419970B4
419975EC 41997688 413DE9A4 413DEA90 413DBCB8 419980C8 407C6D88 41094BC0
$0 : 00000000, AT : 430D0000, v0 : 000081D4, v1 : 41969110
```

```
a0 : 0D0B0D0B, a1 : 47DA86A8, a2 : 47DA86D4, a3 : 47DA86D0
t0 : 47DA86CC, t1 : 47DA86C8, t2 : 47DA86C4, t3 : 47DA86C0
t4 : 47DA86BC, t5 : 47DA86B8, t6 : 47DA86B4, t7 : 47DA86B0
s0 : 00000001, s1 : 47DA86A8, s2 : 507EFE60, s3 : 00000000
s4 : 507EFE60, s5 : 00000000, s6 : 0000001D, s7 : 00000000
t8 : 47DA86F0, t9 : 00000000, k0 : 47EDB5D8, k1 : 41D6F420
gp : 430D96F0, sp : 47EE90B0, s8 : 00000000, ra : 419750CC
EPC  : 41A4686C, ErrorEPC : 41B718D8, SREG     : 3400FF03
MDLO : 00141240, MDHI     : 00000000, BadVaddr : 0D0B15A3
DATA_START : 0x42DB96D0
Cause 80000010 (Code 0x4): Address Error (load or instruction fetch) exception
:
:
```

- CSCsl06059

  Symptoms: Invalid memory access occurs and the routers crash.

  Conditions: The following steps lead to the crash:

  1. Configure a vrf.
  2. Configure a route-map with set ip vrf.
  3. Delete the route-map.
  4. Configure a new vrf.

Note The bug is not reproducible under normal circumstances. The problem can be recreated only via regression (meaning asynchronous) when you try to configure a route-map with the same name which has gone through the deletion process recently.

  Workaround: Configure route-maps with different names.

- CSCsl06110

  Symptoms: Port-channel interfaces are ignored when read from the DHCP snooping database.

  Conditions: When the DHCP snooping database is read in, entries pointing to port channel interfaces are ignored.

  Workaround: There is no workaround.

  Further Problem Description: This is a fairly uncommon case. The database is only read in on a full reload, or if forced manually. In normal operation, port-channel interfaces can be used as DHCP snooping interfaces with no adverse effects.

- CSCsl06336

  Symptoms: When the **maximum-paths** *n* **import** command is unconfigured, for example, a **no maximum-paths** *n* **import** *m* command is issued for a VPN/VRF on a router, sometimes the routes in that VPN may have duplicate path entries.

  For example:

```
diezmil#sh ip bgp vpnv4 v v1001 10.0.20.0
BGP routing table entry for 100:1001:10.0.20.0/24, version 1342275
Paths: (2 available, best #1, table v1001)
Flag: 0x420
```

```
Not advertised to any peer
65164, imported path from 100:1:10.0.20.0/24
  192.168.1.7 (metric 4) from 192.168.1.254 (192.168.1.254)
    Origin IGP, metric 1552, localpref 80833, valid, internal, best
    Extended Community: RT:100:1001
    Originator: 192.168.1.7, Cluster list: 192.168.2.7
    mpls labels in/out nolabel/291
65164, imported path from 100:1:10.0.20.0/24
  192.168.1.7 (metric 4) from 192.168.1.253 (192.168.1.253)
    Origin IGP, metric 1552, localpref 80833, valid, internal
    Extended Community: RT:100:1001
    Originator: 192.168.1.7, Cluster list: 192.168.2.7
    mpls labels in/out nolabel/291
```

Workaround: The least resource-intensive workaround is to configure and unconfigure a dummy import map under that VPN/VRF. Clearing the affected BGP sessions on PEs also resolves the issue.

- CSCsl06515

  Symptoms: Crash is observed on a 13 Slots chassis with 11 eFlexWan with 2 sup720-3bxl. The RP crashes with breakpoint exception.

  Conditions: Crash is observed during boot.

  Workaround: There is no workaround.

- CSCsl07347

  Symptoms: A Cisco 7600 with two RSP720-3Cs has been running fine with multicast traffic. MMLS entries were created and multicast were handled by hardware. After supervisor failover, all multicast traffic may get switched in software due to no MMLS entry was created. It may result in high CPU load temporarily depending on the traffic volume.

  Conditions: This issue is not seen on SUP720s.

  Workaround: There is no workaround.

- CSCsl07424

  Symptoms: VPLS stops packet forwarding via MPLS-TE backup path after MPLS-TE primary path goes down.

  Conditions: The problem is observed when MPLS-TE tunnel has two different paths, one is primary and one is backup, and these two path use the different line card.

  Workaround: **Shut/no shut** tunnel interface.

- CSCsl07623

  Symptoms: The router crashes in certain conditions. No particular user commands are issued.

  Conditions: This issue occurs infrequently when a line card is removed or reset.

  Workaround: There is no workaround.

- CSCsl08912

  Symptoms: Traffic stops when new MAC addresses are learned. This was earlier fixed by CSCsg55237 and reimplemented by CSCsl08912.

  Now problem is fixed, i.e., traffic does not stop when new MAC addresses are learned.

  Workaround: There is no workaround.

- CSCsl10489

  Symptoms: Optimized Edge Routing (OER) feature may choose an exit with a lower Mean Opinion Score (MOS) when current exit has a better MOS. It does not consider the current exit when it selects the best exit based on MOS.

  Conditions: Occurs when MOS is configured as Priority 1 in the OER policy rules for a certain application.

  Workaround: There is no workaround.

- CSCsl11335

  Symptoms: The number of entries obtained from the “ciscoMvpnBgpMdtUpdateTable” table using the **getmany** command is incorrect

  Conditions: Occurred on a Cisco 7200 router running Cisco IOS version 12.4(17.9)T.

  Workaround: There is no workaround.

- CSCsl11549

  Symptoms: A CPUHOG warning is logged for the environment polling process. When this occurs, spanning tree instabilities can be experienced.

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

  Workaround: Disable VTT temperature monitor with the following commands:

  ```
  config terminal
  service internal
  exit
  enable

  remote command switch test env poll disable vtt 1 temp 0
  remote command switch test env poll disable vtt 2 temp 0
  remote command switch test env poll disable vtt 3 temp 0
  ```

- CSCsl12560

  Symptoms: TTL = 1 packets are not forwarded over IP InternetWorking EoMPLS tunnels.

  Conditions: This problem happens only in IP InternetWorking EoMPLS tunnels.

  Trigger: ATOM internetworking is configured on the Cisco 7600 router using the ethernet-atm topology. On the ethernet PE device, EoMPLS is configured.

  Root Cause: Cisco IOS Code Issue.

  Impact: Multicast packets with “TTL value as 1” are getting dropped.

  Workaround: Increase TTL value to 2.

- CSCsl13477

  Symptoms: Traffic will be lost after SSO switchover, for the configuration with GRE/IPSec, and multiple crypto map to one map peer, and GRE is taken over by VPNSPA.

  Workaround: With map to map config or do not have GRE taken over by VPNSPA.

- CSCsl14204

  Symptoms: Standby CPU utilization is 90%. Standby reloads during transition to Active after SSO.

  Conditions: This symptom is seen when redundancy mode SSO with spanning tree is configured in MST mode. This is not specific to SSO. The trigger is “spanning-tree mode mst”. The crash will not happen if the spanning tree is set to PVST. The router reloads.

Workaround: Configure spanning tree in PVST mode.

- CSCsl16127

  Symptoms: Egress classification on SIP600 may not function as expected.

  Conditions: When an egress policy is applied to a SIP600 interface, traffic may be incorrectly classified and may be sent to incorrect queues.

  Workaround: There is no workaround.

- CSCsl17798

  Symptoms: Etherchannel membership on standby supervisor is inconsistent with the state on active supervisor. This is reported in ESM-20G line card.

  Conditions: This defect may be seen with etherchannel mode is “on” and on a standby reload. Reported in Cisco 7600 series router. Could impact other platform as well.

  Trigger: Etherchannel configuration and performing SSO.

  Impact: This may impact traffic forwarding. Etherchannel state inconsistent between active and standby.

  Frequency: Every time when Line card reloads.

  Workaround: Once standby supervisor has reached hot, remove etherchannel configuration and reapply.

- CSCsl18765

  Symptoms: On a Catalyst 6500 or Cisco 7600 router if you configure an xconnect L3 ethernet port as span source of a span session, it can cause the following:

  – Duplication of traffic on the VC.
  – Packet reflected back on the VC leading to CE of the EoMPLS tunnel to disable its port for loopback or spanning-tree reason.
  – Loop between ingress and egress PE.

  Conditions: This bug is about multiple issues when configuring span on a L3 interface configured for xconnect (EoMPLS port based). This is seen with the following Cisco IOS Releases: 12.2(18)SXF7, 12.2(33)SRA4, and 12.2(33)SRB2, but it may impact all releases. The problem is not seen with PFC3C.

  Workaround: Do not span a xconnect port.

  Further Problem Description: This problem impacts all code in both Cisco 7600 and Cisco Catalyst 6500 series switch. This bug can cause a simple monitoring feature to bring down a complete MPLS core network in a matter of seconds.

- CSCsl20133

  Symptoms: When a PE receives E-IGRP derived VPNv4 routes with SoO from other PEs, it does not advertise all the remote VPN routes to a CE.

  This symptom does not occur when CE is running Cisco IOS Releases 12.2(33)SRB or 12.2(40)SE.

  Workaround: Remove sitemap on all the remote PEs if configured. Use prefix-based filtering to avoid routing loop in redundant PE sites instead of SoO.

- CSCsl20559

  Symptoms: When VSI (VLAN) interface is shutdown on a PE, spanning tree loop happens among CE routers.

  Workaround: There is no workaround.

- CSCsl21668

  Symptoms: MPLS packets are punted to RP during tag2tag operation for the Scalable EoMPLS VCs. Scalable EoMPLS is the type of EoMPLS VC where the xconnect is configured on the EVC or on the sub-interface of a SIP-400 line card.

  Conditions:

  – A **shut/no shut** is done on the core facing line card.

  – OIR of the core facing line card.

  Workaround: Decrease the rate of punted packets to RP which will reduce the CPU load to correct the problem.

  Further Problem Description: The tag2tag adjacency on the forwarding engine is programmed as punt which causes packets to be punted to RP. The tag2tag adjacency is programmed as punt because the adjacency is incomplete during OIR or **shut/no shut** operation. Hence, if the traffic to the route processor is reduced, adjacency could be completed by ARP.

- CSCsl25559

  Symptoms: Even with traffic rate underneath the ratio of allowed bandwidth set by Qos, the traffic will be underserviced and some packets will be tail dropped.

  Conditions: None

  Workaround: There is no workaround.

  Further Problem Description: In certain conditions, every time a class of traffic is scheduled, it will gain some “tokens” to be allowed to take advantage of remaining bandwidth (therefore increasing slightly its ratio). There is no CAP on how much it can gain. After a while, the value increases so much that it will overflow. At that point, the traffic class will be constantly rescheduled in a future slot without being handled. We will start building the queue and finally tail drop.

- CSCsl27236

  Symptoms: WS-C6506-E with WS-SVC-IPSEC-1 keeps crashing with error %SYS-3-CPUHOG: Task is running for (126000)msec. This is a CPU HOG SW forced crash. VPN router is failing to Redundant Supervisor.

  Conditions: RP crashes before SUP720. This is seen under stress condition and when IPSEC / ISAKMP is enabled.

  Workaround: There is no workaround.

  Further information: This is a day one bug that just surfaced. The customer found this under heavy stress conditions. The node list is getting corrupted. We will iterate through the list indefinitely causing the CPU hog.

- CSCsl27840

  Symptoms: Router hangs. The router and module may crash.

  Conditions: This symptom is seen in Cisco 7600 router.

  Workaround: There is no workaround.

  Further Problem Description: Some times a router may crash, a PA reset is seen, and the router hangs consistently. High CPU utilization is seen when Shut ATM memberlink with Mlpofr & MLPoA configs with common VT.

- CSCsl27984

  Symptoms: POS interface does not come up after the bootup of a Cisco 7600 router.

Conditions: This issue is seen immediately after the bootup of Cisco 7600 router with POS interface module.

Workaround: Problem is sorted out by removing and attaching the cable and then resetting the POS interface. After this procedure, POS interface comes up and works fine.

- CSCsl29059

  Symptoms: Standby supervisor in Cisco 7600 is reset due to RF Keepalive timeout.

  Conditions: This bug can happen before standby reaches standby hot state and will be seen if standby is in standby config RF progression.

  Workaround: There is no workaround.

- CSCsl30069

  Symptoms: A Cisco Catalyst 6500/7600 might crash due to memory corruption on the Route Processor (RP).

  Conditions: This symptom occurs when running Cisco IOS Release 12.2(33)SRB2 and when BGP is configured on the box.

  Workaround: There is no workaround.

- 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.

- CSCsl41325

  Symptoms: A router crashes when BGP adjacency goes down. Lots of spurious memory access is seen.

  Conditions: This symptom is observed on a Cisco 7600 series router with Supervisor 720-3BXL that is running Cisco IOS Release 12.2(33)SRB2. Multicast routing must be enabled and there must be multiple BGP paths with different preferences to a default route. If the preferred default route goes down this crash may be seen.

  Workaround: Have only a single path to the default route.

- CSCsl41685

  Symptoms: Attaching a hierachical policy with 250 classes to a switchport of an ES-20 fails.

  Conditions: This symptom is seen in scaled configuration with 250 classes, with a child policy in class-default.

  Workaround: There is no workaround.

- CSCsl49167

  Symptoms: Continuous %IPC-5-WATERMARK: 884 messages pending in xmt for the port slot on 7600 SIP400. It affects any type of 7600 chassis and is not Specific to any Sup. The message are warnings that the buffer is being used up.

  Conditions: The problem occurs under high traffic conditions between RP and LC. The underlying EOBC transport encounters lots of collisions, which results in the WATERMARK message.

  Workaround: There is no workaround.

  Further Problem Description: The way it was reproduced was by pumping heavy traffic into IPC and simulating congestion at the driver layer.

- CSCsl49628

  Symptoms: When a VRF is deleted through the CLI, the VRF deletion never completes on the standby RP, and the VRF cannot be reconfigured at a later time.

  Conditions: This symptom is observed when BGP is enabled on the router.

  Workaround: There is no workaround.

- CSCsl49705

  Symptoms: ISSU between SRB-2 & SRB-3 done, with tunnels configured on active, causes “IDBINDEX_SYNC-4-RESERVE” messages on standby (SRB-2) & a delay (wait) of around 3 seconds per tunnel, which causes a standby reset in case there are large number of tunnels configured.

  Conditions: This symptom is seen when tunnels are configured.

  Workaround: Remove tunnels configs before doing ISSU.

- CSCsl50500

  Symptoms: System is reset due to WATCHDOG ERROR.

  Conditions: During heavy stress condition CPU freeze is observed. This is specific to RSP720 hardware. This is a very rare race condition in CPU complex. It was seen only once so far. Not expected to be seen again. Very Rare. A router reload is observed.

  Workaround: There are no workarounds that would guarantee that the problem will not occur. The probability of the occurrence can, however, be lowered by protecting the RP CPU from overload. This can be achieved by enabling MLS rate-limiters or configuring Control Plane Policing.

- CSCsl50569

  Symptoms: A SIP-400 module may drop all ingress packets destined for another fabric-enabled module. Prior to this, the module would be operating correctly.

  Conditions: This problem has only been seen with Cisco IOS Release 12.2(33) SRB2. The exact trigger is still unknown.

  Recovery: To recover connectivity, there are two options. Option 1 is preferable since it causes less traffic interruption. If Option 1 does not work, then Option 2 should be performed. 1. Attach to the switch processor (**remote login switch**) and issue the command: **test fpoe index 0 FFFF restore** 2. Reload the ingress SIP-400 linecard: **hw-module module** *mod* **reset**

  Workaround: To prevent issue from occurring in 12.2(33)SRB2, diagnostics can be disabled on the SIP-400 with the following command: Router(config)#no diagnostic monitor module <slot#> test 1

- CSCsl50774

  Symptoms: Line card crashes repeatedly during boot after an unsuccessful FPD upgrade.

  Conditions: This symptom affects SRB, will prevent the line card from booting.

Workaround: Once the line card is in the problem state, it cannot be recovered without this bug fix.

Further Problem Description: The problem is that the recovery mechanism that is in place to correct for a mis programmed link FPGA needs an update.

- CSCsl51765

  Symptoms :The router crashes on doing a “no t1 channel-group”.

  Conditions: This symptom occurs when the “no channel-group” is issued on a CT3 SPA on a SIP400.

  Workaround: There is no workaround.

- CSCsl52092

  Symptoms: Port channel interfaces in the DHCP snooping database are not read back correctly when the database is refreshed. Either the interface is not recognized and the entry is ignored, or the entry may be assigned to the correct or an incorrect portchannel.

  Conditions: This problem happens in any case when a portchannel interface is found in a DHCP snooping database, and the database is read in.

  Workaround: Use an interface other than port-channel, or do not use the DHCP snooping database.

- CSCsl53494

  Symptoms: The error messages generated for the SSC-400 card display the product name as SSC-600, which belongs to another card.

  Conditions: Log messages on failures.

  Workaround: Correct the product name string.

  Further Problem Description: SSC-600 is the next generation card which is not supported on this branch. The correct name for sxf should be SSC-400

- CSCsl54875

  Symptoms: The “test platform firmware get asic ....” command issued for a module, may reset that module.

  ```
  Messages:
    00:27:15: %PM_SCP-SP-1-LCP_FW_ERR: System resetting module 4 to recover
    from error: Linecard received system exception
    00:27:15: %OIR-SP-3-PWRCYCLE: Card in module 4, is being power-cycled Off
    (Module Reset due to exception or user request)
    00:27:15: %C6KPWR-SP-4-DISABLED: power to module in slot 4 set Off (Module
    Reset due to exception or user request)
  ```

  Conditions:

  - CAT6500 switch or Cisco7600 that is running Cisco IOS Releases 12.2(33)SRB1 or 12.2(33)SRB2.
  - This issue is NOT applicable for Cisco IOS 12.2(18)SXF releases.
  - Affected Modules: WS-X6704-10GE and WS-X6748-GE-TX.

  Workaround: Use “test platform firmware component” to capture ASIC register values.

- CSCsl56547

  Symptoms: While getting the output of the”sh mls cef ipv6 vrf <id>” for a valid existing VRF, error message is seen. % VRFv6 does not exist.

  Conditions: This issue is seen only for IPv6 VRF. If we have both v4/v6 address-family for the VRF then this problem does not happen.

Trigger: This problem is reproducible by two ways:

1. Configure vrf, save the config and reload the box

   Workaround: Configure global command **vtp mode transparent**.

2. Configure VRF and toggle IPv6 unicast-routing.

   Workaround: There is no workaround.

Further Problem Description: Doing a SSO switchover can be used as workaround.

- CSCsl56824

  Symptoms: STP does not block a port and creates network loop after PE router reloads.

  Conditions: This problem is observed when using VPLS.

  Workaround: There is no workaround.

- CSCsl60107

  Symptoms: VPLS/EoMPLS traffic may be dropped at imposition when a WRED policy applied to any port on the same HW datapath on SIP600 or ES20.

  Additionally, QoS may be incorrectly applied and traffic may stop on an FRR cutover of a VPLS/EoMPLS VC under similar conditions to above.

  Conditions:

  1. If a VPLS/EoMPLS VC egresses a port with no QoS applied and any other port on the LC has a WRED policy applied, the VC traffic may be dropped in the imposition direction, or misqueued.
  2. If a VC is FRR protected and both the primary and backup paths egress ports on the second datapath on ES20 (ports 10-19), VC traffic may be dropped on tunnel switchover to the backup path.

  Workaround:

  1. Configure QoS on the egress interface carrying the VPLS/EoMPLS VC.
  2. Configure primary and backup tunnel paths to egress interfaces on the first 10 ports of ES20.

- CSCsl60761

  Symptoms: On reloading the router with scaled QoS configurations, the OSM LC may observe memory fragmentation errors.

  Conditions: QoS configurations should be scaled configs.

  Workaround: There is no workaround.

- CSCsl62346

  Symptoms: Class queue experiences unexpected high packet drops.

  Conditions: This is noticed on Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRB image and later. When a service policy is applied on ATM PVC on SPA-2xOC3-ATM hosted by 7600-SIP-400, the packet drops are unusually high and throughput on the class queue is much less than the expected.

  Workaround: Configure WRED on the class queue by using the **random-detect aggregate** command. Or increase the queue length of the class using **queue-limit** command, but this is inefficient use of buffers.

- CSCsl65335

  Symptoms: A Cisco IOS 6500 or 7600 router that is running WCCP may reload when a WCCP redirect ACL is modified.

  Conditions: The router must be configured for WCCP L2 redirection with mask assignment and input redirection on one or more interfaces. Further WCCP must be configured with a redirect ACL. The reload is triggered when the ACL is updated (modified) at the same time as an appliance is shutdown or fails.

  Workaround: If possible wait for the appliance to shutdown (WCCP-1-SERVICELOST) before updating the ACL.

  Further Problem Description: The reload may be more apparent when the WCCP control protocol is experiencing some instability: numerous WCCP-1-SERVICELOST, WCCP-5-SERVICEFOUND events, or if the appliance is being reconfigured at the same time as the ACL is updated.

- CSCsl69206

  Symptoms: Ping does not pass through GRE tunnel which is a VRF member after 2nd SSO switchover.

  Conditions: This occurs after a stateful switchover has happened twice on the router.

  Workaround: Reload the router.

- CSCsl70148

  Symptoms: On bootup with the 200 Mcast enabled p2p Crypto GRE Config we see that the Tunnels are not installed in hardware and the entries are continuously getting deleted and created. This problem happens on image running Cisco IOS Release 12.2(SX)F12.

  Conditions: No explicit commands are run. This happens when booted with the above configuration.

  Workaround: There is no workaround.

- CSCsl70175

  Symptoms: A router that is running Cisco IOS may crash if a sequence of configuration commands like the following is entered at the prompt:

  router eigrp 101

  redistribute bgp 300

  router eigrp 101

  redistribute bgp 200

  (The crash is not specific to redistribution commands under EIGRP; entering two **redistribute bgp** *AS* commands with different AS numbers anywhere could trigger the crash.)

  Conditions: BGP does not have to be running prior to the **redistribute bgp** *AS* configuration commands being entered. The crash is not specific to any other routing protocol. Entering two BGP redistribution commands with different AS numbers anywhere on the router can trigger the crash.

  Workaround: Check configurations before applying them to the router to be sure that the AS numbers used for all redistribution commands are correct.

- CSCsl70667

  Symptoms: A line card crash is observed after the following error messages:

  ```
  FIBXDRINV: Invalid XDR format. FIB entry XDR has bogus routecount
  ```

  Conditions: This error message and crash are seen very rarely after OIR of the line card.

  Workaround: There is no workaround.

- CSCsl71254

  Symptoms: A Cisco 7609-S router, with RSP720 processor, using ES20 line card, and running Cisco IOS Release 12.2(33)SRB2 crashes.

  Conditions: This symptom occurs when configuring L3 subinterface with dot1Q NATIVE encapsulation on ES20 card interface, where already service-instance configured.

  Workaround: There is no workaround.

- CSCsl71339

  Symptoms: Every couple of days, a Cisco 1000BaseT gigabit interface goes down/down (not connect) unexpectedly. No errors nor logs were observed, a part to the usual sequence of %LINEPROTO-5-UPDOWN:, %LINK-3-UPDOWN:, %LINEPROTO-SP-5-UPDOWN:, %LINK-SP-3- UPDOWN: (if the **logging events link-status** command is enabled on the interface).

  Conditions: This symptom is observed on multiple Cisco 7613 routers that are running Cisco IOS Release 12.2(33)SRB2 and equipped with WS-X6724-SFP + DFC + GLC-T (1000BaseT adapters). Fiber SFPs are not affected. WS-X6748-SFP does not exhibit the symptom.

  Workaround:

  – OIR (unplug and plug back) the GLC-T adapter.

  – These symptoms were never observed with Cisco IOS Release 12.2(33)SRA3, so downgrading may be another workaround, if applicable.

  – If the customer is running a debug image, as a temporary measure, the interface can be recovered by the following sequence: **shut** the interface, then issue the following commands from the line card console:

    ```
    Dfc# test plat debug call name ant_cu_sfp_phy_reset 2  1
    Dfc# test plat debug call name ant_cu_sfp_phy_reset 2  0
    ```

  Then **no shut** the interface where *port#* is the zero-based port number.

  This will reset the copper SFP, which will recover the interface.

  Further Problem Description: To determine if the customer is encountering this issue, log on to the line card console as follows:

  ```
  Router config# service internal
  Router conifg# service slave-log
  Router config# end
  router# remote login module
  Trying Switch ...
  Entering CONSOLE for Switch
  Type "^C^C^C" to end this session
  ```

  Next, capture the output from the following debug command:

  ```
  Router-dfc# test plat firm comp m88e1111 acc dump-cu <port-#>
  ```

Note When accessing the line card debug commands, the ports are numbered starting at 0 (not 1), so: Router-dfc# test plat firm comp m88e1111 acc dump-cu 0 will print the phy registers for (front-panel) port #1.

  If the cu-sfp-phy is working correctly, you will see the values of the cu-sfp-phy registers displayed, and the linecard is not encountering the problem tracked by this bugid.

  On the other hand, if this bug is encountered, the phy registers will be inaccessible and you will see:

"Error reading m88e1111 copper registers on port <port-#> ! "

This issue is resolved in Cisco IOS Releases 12.2(18)SXF14 and later, 12.2(33)SRC and later, 12.2(33)SRB3 and later, and 12.2(33)SXH2 and later.

- CSCsl71540

  Symptoms: Router reloads when the **sh ip bgp** *options* command is entered.

  Conditions: This is seen in releases where CSCsj22187 is fixed.

  Workaround: There is no workaround.

- CSCsl72281

  Symptoms: After a Cisco 7600 series router reloads, host routes created by DHCP relay process for DHCP clients that are connected to unnumbered VLAN interfaces point to wrong VLAN interface.

  Conditions: This symptom occurs when interface-index value parameter on the router changes after the router reloads. This parameter is stored in DHCP bindings database on TFTP or FTP server. It is recalculated in case of the router reloading and may change if a new interface is added or existing interface is removed from the configuration. For example, a single interface VLAN is added to the configuration prior to the router reloading.

  Workaround: There is no workaround.

- CSCsl72774

  Symptoms: A router may run out of memory and fail malloc due to a memory leak.

  Conditions: This problem only occurs on distributed platforms (like the Cisco 7600/Catalyst 6500) when the CEF consistency checkers have been enabled. By default, the CEF consistency checkers are disabled. When the CEF consistency checkers are turned on, memory is leaked on the RP, SP and line cards.

  If you want to use the consistency checkers, then do so for only short periods of time. For example, use the consistency checkers while diagnosing network problems.

  Workaround: Disable the CEF consistency checkers by using the following commands:

  no cef table consistency-check ipv4

  no cef table consistency-check ipv6

- CSCsl72789

  Symptoms: SW_INIT_TIMEOUT message for ES20 line cards, line card may or may not recover.

  Conditions: Generally this error is seen with large routing tables, large configurations with many subinterfaces, or in the case of hardware failure.

  Workaround: Depending on the source of the error, the workaround may be to reload the line card or reload the chassis. Some problems may have no workaround.

  Further Problem Description: This fix will effectively remove the possibility of a SW_INIT_TIMEOUT.

- CSCsl76647

  Symptoms: The **clear crypto isakmp** command deletes SA with connection ID from 0 to 32766. The SA created with the VPN SPA has a connection ID higher than 32766, and cannot be singularly deleted.

  Conditions: This symptom occurs when SA is established using the VPN SPA.

  Workaround: There is no workaround.

- CSCsl77385

  Symptoms: Long delay of RF_PROG_ACTIVE event is observed on Cisco Catalyst 6500 series switch.

  Conditions: This issue was observed during investigation of CSCsl66247.

  Trigger: Cisco Catalyst 6500 series switch MLS Multicast.

  Impact: This long delay caused AToM VCs to not be able to come up after a switchover.

  Workaround: There is no workaround.

- CSCsl78159

  Symptoms: The **no passive-interface** command in OSPF configuration is not synchronized to standby RP. There are no errors reported.

  Conditions: The following sequence of OSPF configuration commands leads to the problem:

  1. **passive-interface default**
  2. **no passive-interface Serial2/0**
  3. **no passive-interface default**

  Workaround: Remove and restore OSPF process configuration.

  Further Problem Description: Here is an example of the difference in active and standby RP configuration:

```
ACTIVE RP:
router ospf 200 vrf test
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
 default-information originate metric 30 metric-type 1
!

STANDBY RP:
router ospf 200 vrf test
 log-adjacency-changes
 passive-interface default
 no passive-interface Serial2/0
 network 0.0.0.0 255.255.255.255 area 0
 default-information originate metric 30 metric-type 1
!
```

- CSCsl79141

  Symptoms: The new AToM VCs that are configured after their line card reset, may not come up.

  Conditions: This happens if those VCs are one-side configured on the remote when the LC resets.

  Workaround: Reconfigure the VCs on both sides will clear the problem.

- CSCsl79195

  Symptoms: Following boot, or reload, of standby supervisor, the XDR_ISSUNEGOFAIL errmsg is seen relating to the standby SP. This can only be seen on a Cisco 6500/7600 as this is specific to the supervisor card.

Conditions: This symptom is only seen if the standby supervisor is reloaded after it has first booted far enough for the XDR peers representing it to have been created on the active RP, but before the platform signals the OIR event for the card. A typical scenario is a transient RF progression failure.

Workaround: Reload the standby supervisor.

- CSCsl79219

  Symptoms: Bidir shadow entries may not be installed in hardware thus blocking the multicast traffic in some conditions.

  Conditions: This symptom occurs on the Cisco Catalyst 6500 switch that is running with MVPN configuration. The core network is in PIM-Bidir mode and sometimes the "z" flag setting for data MDT groups is not populated to hardware.

  Workaround: Use the **clear ip mr** *mdt_group* command to solve the problem.

- CSCsl83211

  Symptoms: Some Sup32 boards running Modular IOS software crash (silently) during bootup after a power-cycle. The root cause was found to be excessive interrupts from the Earl during initialization.

  Conditions: Sup32 running Modular IOS (ION) Power-cycle the switch.

  Trigger: The Earl is generating continuous interrupts at a very high rate, even before the initialization of the earl asics is complete.

  Impact: Normal operation of an Production network.

  Workaround:

  1. Use IOS image.
  2. Do not cold boot the system (i.e. turn off the power). Instead use **reload** command from Cisco IOS prompt or ROMMON prompt.

- CSCsl83415

  Symptoms: After executing the following CLI (steps mentioned alphabetically) via a script (not reproducible manually), the router sometimes crashes:

```
Test10 :
---------
a. clear ip bgp 10.0.101.46 ipv4 multicast out
b. clear ip bgp 10.0.101.47 ipv4 multicast out
Test 1:
-------
c. show ip bgp ipv4 multicast nei 10.0.101.2
d. show ip bgp ipv4 multicast []
e. config t

Crash does not happen for each of the following cases:
1. if same CLI is cut-paste manually, there is no crash.
2. if clear cli is not executed, there is no crash.
3. if config term is not entered, there is no crash.
```

  Conditions: The symptom occurs after executing the above CLI.

  Workaround: There is no workaround.

- CSCsl85847

  Symptoms: Router may reload due to some sup ipc issue. The XDR gets disabled with the line card and the RP-SP IPC communication is broken. External Data Representation (XDR) communication to a line card is disabled, followed by a message in this format:

  ```
  %XDR-6-XDRDISABLEREQUEST: Peer in slot 2/0 (2) requested to be disabled due
   to: XDR Keepalive Timeout. Disabling linecard
  ```

  Conditions: This symptom is observed on Cisco 7600 series routers that are running Cisco IOS Release 12.2(33)SRB under some high XDR traffic conditions. Affected line card can be a SIP card, line card with DFC or SP.

  Workaround: There is no workaround.

  Further Problem Description: Most common cause of high XDR traffic is flap of a routing peer with a high number of advertised prefixes. This will cause a high number of updates to the Forwarding Information Base (FIB), which has to be distributed to SIP cards, line cards with DFC and SP.

- CSCsl89176

  Symptoms: Device will crash.

  Conditions: This symptom happens in all platforms where the device is polling for VLAN information.

  Trigger: vlanTrunkPortEntry is polled via SNMP.

  Frequency: Not applicable.

  Impact: Could not configure LACP max-bundle.

  Workaround: Excluding the polled MIB causing the crash.

  ```
  snmp-server view 1.3.6.1.4.1.9.9.46.1.6.1.1 excluded
  snmp-server community view RO
  ```

- CSCsl89425

  Symptoms: Bidirectional Forwarding Detection (BFD) sessions do not scale. This symptom is especially visible with OSPF client when one of the peers is rebooted after configuring maximum number of BFD sessions.

  Conditions: Occurs when configuring maximum BFD sessions or total number of BFD sessions too close to maximum limit.

  Workaround: Configure 90% of maximum allowed BFD sessions.

- CSCsl90341

  Symptoms: A Cisco 7600 series router that is running Cisco IOS Release 12.2(33) SRB2 does not report all the Netflow flows even though **ip flow ingress** is configured. This happens when the box comes up after reload. Also very few flows are exported to the collector.

  Conditions: This symptom occurs under the following conditions: - Interface NDE is configured in the box - After the 7600 has come up after the reload. - Box has to have SIP-400 LCs.

  Workaround: Configure **ip route-cache flow** on the main interface or configure **no ip flow ingress** followed by **ip flow ingress** on the sub-interface.

- CSCsl93608

  Symptoms: Error messages are observed on the active console when the standby supervisor is booting up. This eventually leads to continuous reload of the standby supervisor.

  Conditions: This symptom happens only when ISIS VRF is configured. Bulk-sync failure due to PRC mismatch.

Issue Verification: The error can be seen by using the **show redundancy config-sync failures prc** command.

Workaround: There is no workaround.

- CSCsl94259

  Symptoms: When applying the service policy on main interface, exceed error message is seen.

  Conditions: This symptom occurs when applying a policy or doing the OIR.

  Workaround: There is no workaround.

- CSCsl94499

  Symptoms: When applying the **mpls ip** under the top configuration mode command, the standby RP may be reset and the active RP generates the following error message:

  ```
  Dec 27 09:14:43.095 PST: %RTMGR-3-TOPO_SYNC_ERR: Failed to duplicate active
  topology on standby.
  (rc=15), id 1E000000 {default:ipv6:base}
  ```

  Conditions: The problem happens on a Cisco 7600 series router when applying the **no mpls ip** top configuration mode command.

  Workaround: Enable the IPv6 routing explicitly via the **ipv6 unicast- routing** command before issuing the **no mpls ip** command.

  Further Problem Description: There is a synchronization (or timing) issue on IPv6 routing shutdown between active and standby RPs.

- CSCsl94621

  Symptoms: For the ATM multi-vlan to VC feature, when the remote end of the link flaps, the spanning tree instance for the VLAN gets lost. Traffic is no longer forwarded.

  Conditions: Link flap when the ATM VC is the only instance of that VLAN in the router.

  Workaround: If there is at least one other port on the same VLAN, spanning-tree remains, and there is no impact. Configure a switchport and allow all VLANs that are in the ATM multi-vlan VC.

- CSCsl95664

  Symptoms: In a Cisco 7600 series router with hundreds of l2 VCs and l3 VRFs configured, after a reload, traffic to the l3 VPN prefixes having aggregate labelS might experience 10-20 minutes of failure before recovering.

  Conditions: This happens only in scaled configurations with hundreds of VRFs and L2 VCs with QoS enabled.

  Workaround: There is no workaround.

  Further Problem Description: After PE reload, all L3VPN traffic destined for aggregate labels takes a long time (20 minutes +) to recover. There seems to be a significant delay in getting the forwarding entries programmed in HW for aggregate labels.

- CSCsm01399

  Symptoms: After a bus idle event on a module, it is expected for the first healthy interface to be shut down as part of the recovery process. On a 67xx 10G module, this interface may remain down and not recover to the original up state after the bus idle recovery routine is finished. The opposite side of that connection may remain up after the event.

  Conditions: Issue only observed after a bus stall on the affected module and only affects the first healthy port on the module. Issue has been observed on Cisco IOS Release 12.2(18) SXF12.

  Workaround:

  - Do not use the first port on the 10GE module, this port can remain admined down. The first port on the module should be healthy and had passed online diagnostics.
  - Issue is not seen on the SXH train.
  - To restore connectivity after issue occurs, execute a **shut/no shut** on the affected interface.

- CSCsm04693

  Symptoms: SRB code has been changed for tunnel interface, where the tunnel interfaces have been upgraded to have encoded with idb identity, but the corresponding changes to transformation functions have not been done.

  This DDTS aims at filling up the transformations to have proper ISSU with other/old images.

- CSCsm06740

  Symptoms: A memory leak occurs when CLI commands are issued, if AAA command accounting is configured.

  Conditions: This symptom occurs under AAA accounting conditions.

  Impact: Memory leak is observed.

  Trigger: The issue is seen when AAA command accounting is configured, for example:

```
aaa accounting update newinfo
aaa accounting exec default start-stop group GROUPINFO
aaa accounting commands 15 default start-stop group GROUPINFO
```

  Workaround: Remove AAA command accounting configuration

- CSCsm06762

  Symptoms: When displaying routes in a routing table, the last update time may sometimes be shown as “7w0d” when the route has recently been updated. For example:

```
router#show ip route 192.168.116.152

Routing entry for 192.168.116.152/30
  Known via "rip", distance 120, metric 1
  Redistributing via bgp 6747, rip
  Advertised by bgp 6747
  Last update from 192.168.117.154 on GigabitEthernet2/5.2583, 7w0d ago
  Routing Descriptor Blocks:
  * 192.168.117.154, from 192.168.117.154, 7w0d ago, via
GigabitEthernet2/5.2583
      Route metric is 1, traffic share count is 1
```

  The following traceback may also be seen:

```
Jan  4 10:42:33.357 ROUTER: %IPRT-3-NDB_STATE_ERROR: NDB state error (BAD
EVENT STATE) (0x00)
192.168.116.152/30, state 7, event 2->1, nh_type 1 flags 4 -Process= "RIP
Router", ipl= 0,
pid= 494
```

  The updated route will no longer be visible in the forwarding plane.

Conditions: In cases where a distance vector protocol is being used (e.g. RIP) and the route goes into holddown state and then comes out of holddown before the flushtimer has expired, the traceback described above may occur.

Workaround: The route can be restored by doing:

clear ip route 192.168.116.152

- CSCsm09338

  Symptoms: Following tracebacks are sometimes seen on a switchover of c7600 router.

  ```
  *Feb 1 19:46:32.132 buc: %C6K_PROCMIB-DFC7-3-IPC_PORTOPEN_FAIL: Failed to open port
  while connecting to process statistics: error code = no such port
  ```

  Conditions: For this symptom to occur, at least one LAN line card should be present in the chassis.

  Workaround: There is no workaround.

- CSCsm09618

  Symptoms: When performing an ISSU upgrade between the 12.2SRB and 12.2SRC images, SIP-400 and ES20 line cards may fail to come online.

  Conditions: The problem occurs when **issu runversion** is run on the active supervisor after **issue loadversion** has completed. Some line cards may fail to come online after the new supervisor comes online.

  Workaround: When the supervisor reaches terminal state for SSO, the user can configure **power enable module** *x* to re-enable the line card.

- 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.

- CSCsm12692

  Symptoms: IPv6 traffic is limited due to the rate-limiters when RP switchover occurs. And **show mpls forwarding-table** command indicates the duplicate label entries for IPv6 at the same time.

  Finally, the limited IPv6 traffic and the duplicated label entries are restored about 10 minutes later.

  Conditions: The issue will be appeared when RP switchover occurs with 6VPE configuration.

  Workaround: There is no workaround.

  Further Problem Description: Additionally, IPv4's entries are working fine and IPv4 traffic is not limited due to RP switchover.

- CSCsm15406

  Symptoms: Spurious memory access is observed when router boot up.

  Conditions: VPLS is configured. Observed in a setup with 4K VFIs and about 8K VCs.

  Workaround: There is no workaround.

  Further Problem Description: This ddts is applicable only to Cisco IOS Release 12.2(33)SRB3. No other release will be impacted.

- CSCsm17213

  Symptoms: Packet loss/connectivity issues in a IPv4 VRF due to traffic being sent to the rate-limiter and the VLAN-RAM table not being installed correctly. This is seen on interfaces which had an IPv6 address configured on it before.

  Conditions:

  – The VRF needs to be configured for 6vPE and IPv4.

  – The 6vPE needs to be removed from the VRF definition by the **no address-family ipv6**.

  Workaround: **Shut/no shut** the VLAN interface.

- CSCsm21728

  Symptoms: A router crashes when CPU_MONITOR between RP and SP messages have not been heard for more than 150 seconds. This is happening with a congested condition that is running on internal EOBC.

  Conditions: This symptom occurs when there are control data burst and congestions at internal EOBC.

  Workaround: There is no workaround.

- CSCsm23764

  Symptoms: Device keeps reloading every 50 minutes.

  Conditions: The issue will only occur if the standby RP gets reloaded while CEF is part-way through syncing initial data to the standby RP, before standby hot state is reached in SSO mode.

  Trigger: Removal or reload of standby before CEF initial sync is complete.

  Impact: This issue affects operations.

  Workaround: Reload active PRE if this issue occurs.

- CSCsm27565

  Symptoms: The following CPUHOG is observed on executing the **show ip route** *protocol* command:

  ```
  *Jan 18 05:44:07.880 GMT: %SYS-3-CPUHOG: Task is running for (2000)msecs, more than
  (2000)msecs (2/1),process = Exec.
  ```

  Conditions: There must be a large number of routes in the routing table (e.g. 300K+ BGP routes), most of which are owned by a protocol other than that which has been specified in the **show** command.

  Workaround: Do not use the *protocol* argument to filter the routes which are displayed. If necessary, display the console output after the fact.

- CSCsm27958

  Symptoms: After upgrading a Cisco 7600 to Cisco IOS Release 12.2(33)SRC, SSO does not come up and router stays in RPR.

  Conditions: Occurs only if the **passive-interface default** command is configured under OSPF.

  Workaround: After upgrade, unconfigure and configure again the **passive-interface default**.

- CSCsm28791

  Symptoms: PFC-based EoMPLS does not have the correct disposition adjacency sometimes on the ESM20G, SIP-600 line card.

  Conditions: This symptom is due to a race condition on the control plane update.

Workaround: There is no workaround.

Further Problem Description: Make sure that the EoMPLS VC is a PFC-based EoMPLS (i.e. it is configured on the sub-interface or the main interface). Make sure that the disposition is done on the ESM20G and SIP-600 line card.

Using the **show mpls l2transport vc** *vcid* **detail** command, get the local label. Get the PFC adjacency using the **show mls cef mpls** *label* command and the **show mls cef adjacency entry** *addr* command. If the MTU is programmed as 65535 and dindex is 0x14, then you are hitting this problem.

- CSCsm28955

  Symptoms: Hierarchical policy is configured on ES20 port. Here, child policy drop rate are shown correctly but parent drop rate is always stays at 0. The child policy drop rate is also double than exceed packet drop. sh policy-map int output shows wrong counters.

  Conditions: Hierarchical policy is configured on ES20 port.

  Workaround: There is no workaround.

  Further Problem Description: The cause is in hqf_update_blt_stats. In this function, we have one condition, if (!HQF_IS_BLT_FLAG_SET(hqflayer->blt[i], HQF_PRIORITY_ENABLED)) {hqf_stats->dropcount += hqf_blt_stats->dropcount; hqf_stats->dropbytes += hqf_blt_stats->dropbytes;} means if we have priority configured in child, we skip dropcount calculation for parent. In fact, for ES20, we maintain blt for individual class so, need to collect dropcount for that blt. Another thing in this function is, blt structure is initialize to zero, which is also wrong.

  As for ES20 hardware we maintain separate queue for each class we should not skip drop counts for parent class. Removed the condition from hqf_update_blt_stats so, counters are displayed correctly. The DDTS CSCek75359 will be used for double commit to fix double drop rate issue in child policy. Fix is same as existing code in autobahn76.

- CSCsm30584

  Symptoms: the CWPA2 card and device crash after attaching and removing service policy.

  Conditions: Here, V-temp is configured with service-policy. Now, try to apply policy on pvc. In sh policy-map int outout both the policies are active under V-access. Now remove the policy from V-temp and do **shut/no shut** on main or sub-int or reload the module.

  Workaround: There is no workaround.

  Further Problem Description: The regression is N, since there is no passed logs for the tests.

- CSCsm32555

  Symptoms: On a Cisco 7600 router, connectivity from a MPLS VPN to a GRE peer might fail due to inconsistent VPN ID programming.

  Conditions: When Toggle “[no] mls mpls tunnel-recir” command over VRF-aware GRE tunnel config, connectivity might fail.

  Workaround: There is no workaround.

- CSCsm33193

  Symptoms: BGP convergence for 1->2 and 2->1 is not improving even if “cef table ... convergence speed” is enabled.

  Conditions: Combination with L3VPN and L2VPN.

  Workaround: There is no workaround.

Further Problem Description: There is an improvement in BGP convergence (at 2.5 seconds) if we reduce the ISIS prefixes to 2K. Otherwise we get around 5 sec convergence time.

- CSCsm38142

  Symptoms: Potential memory leak on 7600 RP due to software defect in 12.2SRB.

  Conditions: It is observed if any QoS policy (service-policy command) is configured on router. It only impacts distributed platform such as Cisco 7600.

  Workaround: As there is no workaround available, eventually the router could exhaust all available memory and impact router's functionality.

- CSCsm39159

  Symptoms: ARP HA CPU tracebacks may be seen on the STANDBY PRE while it is booting up.

  Conditions: This symptom is seen under extreme cases of large ARP tables. The Cisco 10000 router could generate ARP HA tracebacks on the STANDBY PRE while it is booting up.

  Workaround: There is no workaround.

- CSCsm39609

  Symptoms: When hqos is applied on switchport, with bandwidth in the parent class (no shape) then there is no new sublink allocated for this parent but it shares the default sublink of the port.

  Conditions: This symptom is seen with Hqos with only bandwidth on parent.

  Workaround: There is no workaround.

- CSCsm42758

  Symptoms: A CPUHOG warning is logged for the environment polling process for VTT devices.

  Conditions: Problem seen during VTT device reading. CPU hogs can affect L2 protocols, e.g- Link flaps. This affects RSP720 router only.

  Workaround: Disable VTT temperature monitor with the following commands.

```
config terminal
 service internal
 exit
 enable

 remote command switch test env poll disable vtt 1 temp 0
 remote command switch test env poll disable vtt 2 temp 0
 remote command switch test env poll disable vtt 3 temp 0
```

- CSCsm43482

  Symptoms: The traffic on a VC may be dropped on ingress PE in VPLS network during the other VC goes down in different Vlan. The VC state is up on affected VC during this problem.

  This problem can be restored with **shut/no shut** in target SVI interface on PE.

  Workaround: There is no workaround.

- CSCsm43938

  Symptoms: Standby PRE might reset at bootup while trying to sync over large ARP tables from the primary to the standby PRE.

  Conditions: The issue has been seem with very large (12 MB) configurations and large ARP tables (16K entries). The issue is only seen when the standby is booting up to standby mode.

Workaround: There is no workaround.

- CSCsm43961

  Symptoms: Router with BGP enabled may crash due to memory corruption.

  Conditions: A heavily loaded router CPU as well as a large number of BGP attribute entries used by BGP paths increases the chances of hitting this bug.

  This is observed on Cisco 7600 that is running Cisco IOS Release 12.2(33)SRB2. The issue was observed 5 days after upgrade to Cisco IOS Release 12.2(33)SRB2.

  Workaround: There is no workaround.

- CSCsm44017

  Symptoms: QoS is not taking effect for about 5 minutes due to high LC CPU utilization.

  Conditions: This symptom occurs when there is a dynamic change in the policy-map.

  Workaround: There is no workaround.

- CSCsm44720

  Symptoms: OSPF sham-link does not come up on the Cisco RSP720 supervisor.

  Conditions This will only be observed when the aggregate label is recirculated in hardware. When the aggregate label is in VPN-CAM this issue will not be observed. The **show mpls platform vpn-vlan-mapping** command can be used to check whether the aggregate label is on VPN-CAM (superman) or not.

  Workaround: If QoS is configured which causes the aggregate label to be programmed in TCAM, then remove the QoS.

  Further Problem Description: There is a chance that the RP will crash if the sham-link is configured with the aggregate label is recirculated. It is advisable to remove sham-link in that scenario.

- CSCsm46290

  Symptoms: WRED does not take effect on the remarked CoS value.

  Conditions: If a policy-map marks the CoS field in the packet and also does WRED on the traffic classified in the same class, then WRED does not take effect on the newly marked CoS value.

  Workaround: There is no workaround.

- CSCsm46903

  Symptoms: %SPA_OIR-3-SW_INIT_TIMEOUT: subslot <slot>/<bay>: SPA initialization is not completed, followed by a SPA Bay recovery. %SPA_OIR-3-RECOVERY_RELOAD: subslot <slot>/<bay>: is attempting recovery by reloading SPA.

  Conditions: This symptom occurs in a heavily loaded system with 16K xconnects and around 200K BGP routes, with traffic running, at times on LC OIR. LC fails to come up throwing a SPA Init timeout error.

  Workaround: LC OIR.

- CSCsm47544

  Symptoms: Software/SVI-based EoMPLS with VC type Ethernet VLAN with SIP200, Flexwan, and Enhanced Flexwan as core-facing line cards does not work.

  Conditions: Configure xconnect SVI-based VLAN interface with MPLS core-facing line cards SIP200, Flexwan, or Enhanced Flexwan. If the pseudo-wire VC type negotiated with peer is type 4/Ether Vlan, packets are sent across pseudo-wire with DOT1q VLAN tag removed causing ping to fail between CEs

Workaround: SIP-400, SIP-600, ES20, PWAN2 line cards as core-facing line cards do not have the problem.

- CSCsm49214

  Symptoms: SM20G:LC crash on remove parent input vlan range class in s/w EoMPLS.

  Conditions: Let the traffic be flowing & remove a parent class that matches this traffic in vlan based EoMPLS setup with MIV policy.

  Workaround: Stop the traffic, remove the class-map, resume the traffic.

- CSCsm49865

  Symptoms: A message such as below gets displayed continuously:

  ```
  SRB02:VDB [301] state invalid. Retrying the event
  ```

  Conditions: The system can get in this condition if an interface is flapped.

  Workaround: There is no workaround.

- CSCsm50309

  Symptoms: Border router crashes configuring OER due to a heartbeat failure. We can also observe lots of spurious access, disabling hardware switching to enable netflow aggregation export, high CPU, and the generation of CPU monitor messages, resulting in the device reloading.

  Conditions: Configuring OER in a border router, after perform the command **master IP key-chain password** command when the master becomes up then it enable netflow aggregation export v9 and the CPU got hang (no message sents) and crashes due to a heartbeat failure.

  Workaround: There is no workaround.

- CSCsm51333

  Symptoms: A policy-map with MIV matching on an input vlan and another class-map matching on multiple input VLANS where one of them match on the vlan already present in the other class, then classification is wrong. The overlapping class matches the input vlan for which a class-map is already exclusively defined.

  Conditions: The policy-map needs to have two classes where some of the match input VLANS should overlap. This policy-map is applied in output direction on the core facing interface on an EoMPLS setup.

  Workaround: There is no workaround.

- CSCsm51729

  Symptoms: After a router has been running continuously for more than 7 weeks, the last update time for routes in the routing table will be shown as “7w0d” when the route has recently been updated. For example:

  ```
  router#show ip route 192.168.116.152


  Routing entry for 192.168.116.152/30
    Known via "rip", distance 120, metric 1
    Redistributing via bgp 6747, rip
    Advertised by bgp 6747
    Last update from 192.168.117.154 on GigabitEthernet2/5.2583, 7w0d ago
    Routing Descriptor Blocks:
    * 192.168.117.154, from 192.168.117.154, 7w0d ago, via
  GigabitEthernet2/5.2583
  ```

```
      Route metric is 1, traffic share count is 1
```

The following traceback may also be seen:

```
Jan  4 10:42:33.357 ROUTER: %IPRT-3-NDB_STATE_ERROR: NDB state error (BAD
EVENT STATE) (0x00)
192.168.116.152/30, state 7, event 2->1, nh_type 1 flags 4 -Process= "RIP
Router", ipl= 0,
pid= 494
```

If the traceback is seen, the updated route will no longer be visible in the forwarding plane and will not be redistributed.

Conditions: The router must be running continuously for 7 weeks.

Conditions for the traceback to occur:

- Router must be running continuously for at least 7 weeks.
- A distance vector protocol is being used (e.g. RIP), and the route goes into holddown state and then comes out of holddown before the flushtimer has expired.

Workaround: In the event of traceback, the route can be restored by doing the following:

clear ip route 192.168.116.152

The clear will NOT correct the update time on the routes, which will still be seen as 7w0d. The latter condition can only be cleared by either:

1. Rebooting the router.
2. If redundant RPs are present, reboot the Standby RP, achieve SSO state, and force a switchover.

Either technique will provide another 7 weeks before either of the problems might be encountered again.

- CSCsm53392

  Symptoms: Line card is power cycled because FIB is disabled on the line card. When this happens the following error message is generated:

  ```
  %FIB-2-FIBDISABLE: Fatal error, slot 2/0 (2)
  %SNMP-5-MODULETRAP: Module 2 [Down] Trap
  %OIR-SP-3-PWRCYCLE: Card in module 2, is being power-cycled off (FIB disabled on the
  line card)
  ```

  Conditions: FIB can be disabled on a given line card because of various regions such as the software error or due to platform transport error.

  Workaround: When FIB disable occurs the only way to recover from the issue is to perform an OIR. After the changes made by this change request the line card will be automatically reloaded. If user wants to disable the automatic reload of the line card, the following command needs to be configured on the router:

  platform cef linecard fib-disable action none

  Further Problem Description: If user has configured the command **platform cef linecard fib-disable action none** on the router and performs an ISSU upgrade or downgrade to an release where the command is not supported then the MCL errors will be observed. This will cause the ISSU operation to fail. User is advised to remove the above command while performing the ISSU operation.

- CSCsm53489

  Symptoms: Following recovery, all traffic for a VC is lost. All imposition EoMPLS entries are missing on core-side SIP-400 LC. The traffic doesn't switch back to the primary TE-FRR tunnel on SIP400 from Backup tunnel on other line card.

  Conditions: The problem is seen in 122srb3

  Workaround: Toggling the primary tunnel. On the primary tunnel doing **shut** and then **no shut** switches the traffic back to the primary tunnel from backup tunnel.

  Further Problem Description: For the TE-FRR scenario in which SIP-400 is the primary/protected core-side interface, and other line card is the backup FRR LC/interface; traffic for s/w EoMPLS and VPLS is not restored following a failover and re-optimization. It appears that s/w EoMPLS/VPLS core-side imposition entries do not exist on the SIP-400 line card after reoptimization.

- CSCsm54548

  Symptoms: IP prec to exp bit marking does not work.

  Conditions: This problem is hardly seen in most routers. If the LC is reset abruptly by SP after the router is reloaded, there is a possibility that you might see this issue.

  Workaround: Toggle "mlq qos" off and on if you notice the problem.

- CSCsm56562

  Symptoms: On a Cisco 7600 SIP-400, if a subinterface with no ip address assigned to it is created and then deleted, on the other dot1q subinterfaces connectivity to the neighbors is lost.

  Workaround: Doing a **shut/no shut** on the main interface will fix the problem.

- CSCsm58677

  Symptoms: There might be malloc failures at FW/SIPx cards pointing to PROCMIB process.

  Conditions: These are seen under heavily loaded EOBC conditions. No straight forward trigger.

  Workaround: There is no workaround.

- CSCsm59499

  Symptoms: TOOBIG error msgs are being displayed on the console

  Conditions: The problem is seen on Cisco 7600 router that is running Cisco IOS Release 12.2(33)SRB image when ES20 line card is OIRed. The fix committed for this issue is only the debug fix which will display more information on the error.

  Workaround: There is no workaround.

- CSCsm60223

  Symptoms: Crash may occur with error massage in the log:

  ```
  %SYS-6-STACKLOW: Stack for process Per-Second Jobs running low, 0/9000 prior to crash.
  ```

  Conditions: mpls pal and netflow configured

  Workaround: There is no workaround.

  Further Problem Description: Breakpoint exception, CPU signal 23, PC = 0x42789538

- CSCsm62748

  Symptoms: Issue is seen on ES20 line cards with MPB configuration on EVC. Traffic on bridge domain is flooded and may be sent out on incorrect EVCs instead of being dropped by the filtering code.

  Conditions: Issue seen with MPB configuration on EVC, generally may be seen with VLAN range encapsulation on the EVC.

Workaround: There is no workaround.

- CSCsm64643

  Symptoms: IPv6 prefixes for passive-interface are not advertised by ISIS.

  Conditions: The problem is seen with RSP720 card and only when the **passive-interface loopback0** command is used under the ISIS configuration.

  Further Problem Description: This configuration works properly with SUP720 but not with RSP720.

  Workaround: There is no workaround.

- CSCsm65584

  Symptoms: There is a system convergence delay with scaled config.

  Conditions: With extensive traffic on EoBC bus, RSP720 dual supervisor setup experiences excessive collisions. These excessive collisions result in EoBC packet drop and thus resulting in IPC retransmission. This retransmission affects the convergence time.

  Workaround: There is no workaround.

- CSCsm66228

  Symptoms: LC crashes while booting up. There will be below error message to identify this issue:

  ```
  "Hardware or Software error occurred on Subslot 0. Reason : Fugu: RXHSPITSTATOOF
  Automatic Error recovery initiated. No further intervention required."
  ```

  Conditions: One of ESM20 ports should not have XFP.

  Workaround: Insert valid XFP in two ports slot on ESM20.

- CSCsm66774

  Symptoms: When a MIV policy-map is attached to the core facing interface in the output direction then classification is incorrect.

  Conditions: Apply MIV policy-map to core facing interface in output direction.

  Workaround: There is no workaround.

- CSCsm69368

  Symptoms: Memory allocation failures and WATERMARK messages are seen on console.

  Conditions: Netflow Data Export (NDE) is enabled with Netflow TCAM overflown with flows on a DFC. RP CPU utilization is high.

  Workaround: The system is not supposed to scale for that many flows. Disable Netflow for immediate fix.

- CSCsm71592

  Symptoms: In an MPLS environment the imposition traffic does not recover and is dropped on this router itself. Disposition traffic is going through fine.

  Conditions: This problem is observed after SSO switchover. This problem is observed internally when 600 Scale EoMPLS VCs are configured on the ES20 card as the CE facing link. 600 TE tunnel head ends are configured on this box. Each EoM VC is mapped to a different TE tunnel using the AToM tunnel select feature. Bidirectional traffic is going through this setup. The drop is due to the ADJ incomplete. It did not clear when the next ADJ update was received.

  Workaround: There is no workaround.

- CSCsm72245

  Symptoms: ESM20 crashes when recopying startup config to running config.

Conditions: Reapplying the startup config to running config, after router boots up.

Workaround: There is no workaround.

- CSCsm72807

  Symptoms: The following message is seen:

  ```
  Dec 16 04:53:21: %DHCP_SNOOPING-3-DHCP_SNOOPING_INTERNAL_ERROR: DHCP Snooping
  internal error, Unknown dhcp message type packet should be already handled so they
  should not come here, they will be dropped. -Traceback= 405B938C 405B98D0 406125EC
  41FE7E6C 41FE7D8C 41FE8940 41FE8A90
  ```

  For each such message that appears, a random packet may be corrupted.

  Conditions: This happens with DHCP snooping configured with SSO. This will only happen on the Cisco 7600 and will only happen under stressful conditions

  Workaround: Use RPR+ instead of SSO.

- CSCsm75642

  Symptoms: Ping does not pass through GRE tunnel which is a VRF member after 2nd SSO switchover.

  Conditions: This occurs after a stateful switchover has happened twice on the router.

  Workaround: Reload the router.

- CSCsm77173

  Symptoms: Traffic stops after a policy with marking in user defined classes queueing in class-DFLT is applied to a sub-interface.

  Conditions: Occurs when the above type of policy is applied.

  Workaround: Perform a “shut/no shut” of the sub-interface, then perform a false update of the policy map. For example, set the “class” parameter to the same value in the policy map.

- CSCsm78735

  Symptoms: This is seen during a software reload of the chassis.

  Conditions: Traffic is running in the testbed, and the router reloads. When the device comes back up, the router starts logging tracebacks. It crashes when **clear mpls ldp neighbor *** command is issued, but has also crashes without this command being issued.

  Workaround: Reload the router again, and issue appears to clear.

- CSCsm80847

  Symptoms: In SwEoMPLS scenario, a policy-map on the core facing ES20 interface matching on MPLS experimental topmost does not work.

  Conditions: The core facing ES20 interface should be first having a policy-map matching on input VLAN and then after removal of it and application of a policy-map matching on input VLAN would lead to this condition.

  Workaround: If the policy-map matching on MPLS experimental topmost bits was applied to the core facing ES20 interface without prior application of a policy-map matching on input VLAN, this condition will not be hit.

- CSCsm82449

  Symptoms: EVC stats not incrementing after SSO switchover.

  Conditions: SSO switchover is done with EVCs configured and switching traffic. Post SSO the stats do not increment.

Workaround: Remove and apply the EVC configs.

- CSCsm83812

  Symptoms: The crash has been observed at various time, but mostly while testing private images. While processing non conformance session it crashes. This is due to the stale seat. This could happen during the RMI, process was suspended and other process removed the seat.

  Conditions: The following steps were taking to reproduce the issue:

  1. Toggle bgp (around 440k) routes.
  2. Reset dfc enable line card (3-4).

  Workaround: There is no workaround.

  Further Problem Description: The following are the most common traceback before crash:

```
Router-2#test platform debugger address2sym 89A74B0 89A7628 A6FCC9C
A6F2AF4
0x89A74B0  ---> ipc_process_nonconf_sess_on_seat+F4
0x89A7628  ---> ipc_service_nonconf_session_process+FC
0xA6FCC9C  ---> ppc_process_dispatch+24
0xA6F2AF4  ---> task_execute+28
Router-2#
```

- CSCsm86236

  Symptoms: The standby RP reloads continuously.

  Conditions: On a router in the SSO mode, the **no address-family** *name* command is followed rapidly by a **address-family** <*name*> command in the "vrf definition" sub-mode.

  Workaround: Wait for a few seconds to reconfigure the address-family after de-configuring it.

- CSCsm88279

  Symptoms: Line card fails to boot when there are routes in the routing table.

  Conditions: None.

  Workaround: There is no workaround.

  Further Problem Description: This problem is not seen all the time. It is seen very rarely with a large routing table.

- CSCsm88496

  Symptoms: MPLS disposition traffic on ESM20 may get dropped by EARL.

  Conditions: This symptom is seen with scaled EVC and VPLS/EOMPLS configuration, after several LC OIR events and then an SSO.

  Workaround: Toggle MPLS configuration on the interface that has the issue.

- CSCsm88513

  Symptoms: A router crashes. The crash is seen on Cisco RSP720 and SUP720 setups during bootup.

  Conditions: This crash is because of wrong DDTS commit of DDTS: CSCsd93294.

  Workaround: There is no workaround.

  Further Problem Description: The crash is seen on Cisco 7600 and Cisco 10000 series routers also and is not specific to these platforms.

- CSCsm91084

Symptoms: Link flaps may be observed on a TenGigabitEthernet interface with XENPAK-10GB-LW under load.

Conditions: This symptom is observed under a high-traffic test scenario of over 9 Gb traffic rate through the xenpaks.

Workaround: The XENPAK-10GB-LW will not support over 9Gbps of traffic.

- CSCsm92389

  Symptoms: With "switchport mode dot1q-tunnel" configured, if a user explicitly configures "spanning-tree bpdufilter disable", on an interface flap or an interface **shut/no shut**, "spanning-tree bpdufilter disable" configuration will be replaced with "spanning-tree bpdufilter enable".

  Conditions: This bug happens with dot1q-tunnels and on **shut/no shut**.

  Workaround: Reapply "spanning-tree bpdufilter disable".

- CSCsm94385

  Symptoms: Netflow entry left as part of residue in a diagnostic test.

  Conditions: This symptom is observed on a fully loaded chassis with ESM20G 2X10GE and 20X1 and is seen to leave a net flow entry as a residual of the test due to which traffic is getting disturbed.

  Workaround: A temporary fix is provided by skipping the test from the diagnostic suite.

- CSCso02266

  Symptoms: A Cisco 7600-SIP-600 may crash when carrying a EoMPLS or VPLS VCs over TE/FRR tunnels.

  Conditions: Crash may be observed when the primary TE path goes down.

  Workaround: Avoid TE/FRR configuration for EoMPLS/VPLS VCs on sip600.

- CSCso14979

  Symptoms: Distributed CEF gets disabled for a line card.

  Conditions: This can happen for a few reasons, some of which are:

  1. Heavy IPC load leading to backplane congestion causing timers (started to monitor distribution) to time out.
  2. Breakdown of IPC communication between the RP and the linecard.
  3. Lack of memory to install FIB updates on the linecard

  Workaround: The only way to restart distributed CEF for the disabled line card is by resetting or OIR the line card.

- CSCso25936

  Symptoms: HQoS policy-map does not take effect for 10 minutes after line card (ESM20) OIR.

  Conditions: This symptom occurs after line card OIR when the HQoS policy has been applied to an interface.

  Workaround: There is no workaround.

- CSCso29361

  Symptoms: The commands given in interface range may not be synced to all the interfaces configured in the range in the standby.

  Workaround: There is no workaround.

- CSCso30946

Symptoms: Line card does not come up first time with image download failure with the following error message:

```
%ONLINE-SP-6-DNLDFAIL: Module <slot>, Proc. 0, Runtime image download failed because
of scp send failure
```

Conditions: This is mainly seen when multiple line cards are removed and inserted at the same time.

Workaround: There is no workaround.

- CSCso35876

  Symptoms: Supervisor or DFC line card crashes in cmfi_qos_walk_apply_func.

  Conditions: It is seen very rarely.

  Workaround: There is no workaround.

  Further Problem Description: When this problem is observed, collect the crashinfo from the Supervisor Processor (SP) or the DFC line card.

- CSCso39444

  Symptoms: SP/LC might crash after SSO cutover

  Conditions: This problem is timing issue and would be more easily seen in SSO cutover case.

  Workaround: There is no workaround.

  Further Problem Description: The new Active supervisor will crash after SSO switchover. This is observed consistently on the Cisco test router in the lab.

- CSCso39553

  Symptoms: ESM20 crashes in sip10g_tcam_fm_delete_tcam_entries.

  Conditions: This symptom is seen on a scaled configuration. Copy again the same config from disk to running config leads to this crash.

  Workaround: There is no workaround.

- CSCso50383

  Symptoms: In a Cisco 7600 ring topology with TE-FRR configuration, traffic might get software switched if the packet comes in on a interface and goes out of the same interface.

  Conditions:

  This can happen in a topology like the following:

  R1 ---------- R2 ---------- R3 | | |---------- R4 ----------|

  Link between R3 - R4 is protected via R3 -> R2 -> R1 -> R4 (typical ring topology). R1 and R3 are the end points of a VC. Normally traffic will take the primary TE tunnel via R-> R4 -> R1. When R3 -> R4 link is shut, traffic will go on the back tunnel, R3 -> R2 -> R1 -> R4. In R4, traffic will be sent back on the incoming interface to R1, VC destination. Now in R4 traffic will get punted to RP and route cached.

  Workaround: There is no workaround.

  Further Problem Description: These drops also ignore QoS markings and affect all service classes.

- CSCuk61910

  Symptoms: A PE router crashes while configuring MVPN.

  Conditions: This symptom occurs when MVPN is being configured on a PE router.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRB2

Cisco IOS Release 12.2(33)SRB2 is a rebuild release for Cisco IOS Release 12.2(33)SRB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRB2 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCef77265

  Symptoms: A router may crash upon receiving certain TACACS+ packets.

  Conditions: This symptom is observed when the TACACS+ packets have the length of their headers set to zero.

  Workaround: There is no workaround.

- CSCeh12411

  Symptoms: A router may hang when you enter the **show running-config** command.

  Conditions: This symptom is observed on a Cisco 7200 series but appears to be platform-independent.

  Workaround: Do not enter the **show running-config** command.

- CSCei62358

  Symptoms: A router may crash when a privilege-level 15 user logs on with the callback or callback-dialstring attribute.

  Conditions: This symptom is observed on a Cisco 805 that runs Cisco IOS Release 12.3(15) and on a Cisco 7600 series that has an RSP720 and that runs Release 12.2 (33)SRB1 when the following conditions are present:

  - The router is configured with AAA authentication and authorization.
  - The AAA server runs CiscoSecure ACS 2.4.
  - The callback or callback-dialstring attribute is configured on the AAA server for the user.

  Workaround: Do not configure the callback or callback-dialstring attribute for the user.

  Alternate Workaround: If the callback-dialstring attribute is used in the TACACS+ profile, ensure that the NULL value is not configured for the callback-dialstring attribute.

- CSCek68473

  Symptoms: A router may reload unexpectedly when you reconfigure the **login block-for** command.

  Conditions: This symptom is observed happens after a couple of invalid login attempts have occurred and then you reconfigure the **login block-for** command.

  Workaround: There is no workaround.

- CSCek73197

  Symptoms: The SNMP server engine ID is not removed after you have entered the **no snmp-server engineID** command. This situation can be verified in the output of the **show running-config | inc snmp-server** command.

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

  Workaround: There is no workaround.

- CSCse98807

  Symptoms: A “%SCHED-3-STUCKMTMR” error message and traceback may be generated during the “SNMP Timers” process.

  Conditions: This symptom is observed when there are too many RMON collection events and alarms. The error message and traceback may also be generated when many entries/rows are created in certain MIBs and occur because of simultaneous row creation timeouts.

  Workaround: Ensure that there are not too many RMON collection events and alarms or simultaneous row creation timeouts. However, note that the error message and traceback do not have an impact on the functionality of the platform. The messages are just warning messages from the Cisco IOS process scheduler, indicating that the process (in this case the “SNMP Timers” process) is not able to process all the events before the process suspends.

- CSCsg03830

  Symptoms: The **tacacs-server directed-request** command appears in the running configuration when is should be disabled. When you disable the command by entering **no tacacs-server directed-request** and reload the router, the command appears to be enabled once more.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for CSCsa45148, which disables the **tacacs-server directed-request** command by default.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsa45148. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Temporary Workaround: Each time after you have reloaded the router, disable the command by entering **no tacacs-server directed-request**.

- CSCsg21398

  Symptoms: The Cisco IOS software image may unexpectedly restart when a crafted “msg-auth-response-get-user” TACACS+ packet is received.

  Conditions: This symptom is observed after the Cisco platform had send an initial “recv-auth-start” TACACS+ packet.

  Workaround: There is no workaround.

- CSCsh36727

  Symptoms: IP SLA MPLS path discovery may not properly discover the number of equal-cost MPLS paths between the router on which the IP SLA MPLS path discovery originates and the router that is the target of the path discovery request.

  Conditions: This symptom is observed when an IP SLA MPLS path discovery request is issued on a router for a target IP address and when some of the equal-cost paths between this router (that is, the originating router) and the target router traverse another router on which a single interface provides a connection to multiple downstream neighbors.

  Workaround: Do not use a single interface to connect to multiple downstream neighbors. Rather, use separate interfaces to connect to each of the downstream neighbors.

- CSCsh41142

  Symptoms: A router may crash when you unconfigure and reconfigure a RADIUS server.

  Conditions: This symptom is observed on a Cisco router when you first create 5000 PPPoE sessions in a load-balancing environment, clear the sessions, unconfigure a RADIUS server, and then reconfigure a RADIUS server.

The following example shows the unconfiguring and reconfiguring of the RADIUS server:

```
no radius-server host <ip-address 1> auth-port 1645 acct-port 1646 key <string>
no radius-server host <ip-address 2> auth-port 1645 acct-port 1646 key <string>
radius-server host <ip-address 3> auth-port 1814 acct-port 1815 key <string>
```

Workaround: There is no workaround.

- CSCsj02971

  Symptoms: The **show ip cache aggregation as** command may not function properly.

  Conditions: This symptom is observed on a Cisco 7600 series. When a flow to or from a Cisco ASN Gateway is equal to or larger than 2^16, the output of the **show ip cache aggregation as** command may show the flow as a negative number because a signed 16-bit integer is not properly used or displayed.

  Workaround: There is no workaround.

- CSCsi48975

  Symptoms: A router may crash during the allocation of memory for subflows at the interrupt level.

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

  Workaround: Do not collect subflows such as BGP or IPM.

- 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 whenever 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 a Cisco IOS software image 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.

- CSCsj72320

  Symptoms: A Cisco 7613 may crash during an SNMP dump, causing a memory allocation failure.

  Symptoms: This symptom is observed when you perform an SNMP dump by using an SNMP monitoring tool. The application queries the IP Tunnel MIB and CISCO-SWITCH-ENGINE-MIB on the router, causing a memory allocation failure, preventing the router from completing a SSO and creating a crashfile on the RP.

  Workaround: Remove the IP Tunnel MIB by entering the **remove tunnel mib** command.

Interfaces and Bridging

- CSCsf20714

  Symptoms: A DHCP relay may crash at the “print_unaligned_summary” function while requesting an IP address from a DHCP client.

  Conditions: This symptom is observed on a Cisco router after the bridge group has changed from one group to another.

  Workaround: There is no workaround.

- CSCsj57084

  Symptoms: Voice packets that are processed through a priority queue may be subjected to jitter.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with an Enhanced FlexWAN Module (WS-X6582-2PA) and a PA-A3-T3 port adapter.

  Workaround: There is no workaround.

- CSCsk28821

  Symptoms: A router may reload unexpectedly when you configure 34 or more double-tagged dot1q QinQ subinterfaces.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB or Release 12.2(33)SRB1.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCei93768

  Symptoms: A Cisco router that is configured for BGP may crash and generate the following error messages:

  (Note that the hex values of tracebacks and other parameters that are part of the error messages will vary with different occurrences of the symptom).

```
%SYS-2-NOTQ: unqueue didn't find 4552953C in queue 454BE738
-Process= "BGP Router", ipl= 0, pid= 195
-Traceback= 4063BE54 4099DC2C 40C60FDC 40C6188C 40C627C8 4191C694 40C628BC 40C3BA10
40C3CCE0
%SYS-2-NOTQ: unqueue didn't find 455294EC in queue 454BE690
-Process= "BGP Router", ipl= 0, pid= 195
-Traceback= 4063BE54 4099DC2C 40C60FDC 40C6188C 40C627C8 4191C694 40C628BC 40C3BA10
40C3CCE0CMD: 'end'
```

```
%SYS-5-CONFIG_I: Configured from console by console
%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header,
chunk 45519C14  data 4552953C  chunkmagic 15A3C78B  chunk_freemagic 0
-Process= "Check heaps", ipl= 0, pid= 6
-Traceback= 4063C5FC 4063C788 4065A9D0

chunk_diagnose, code = 2
chunk name is IP RDB Chunk

current chunk header = 0x0x4552952C
data check, ptr = 0x0x4552953C

next chunk header = 0x0x4552957C
data check, ptr = 0x0x4552958C

previous chunk header = 0x0x455294DC
data check, ptr = 0x0x455294EC
```

Conditions: This symptom is observed mostly with configuration changes that involve the **bgp dmzlink-bw** command for a BGP IPv4 address family, but in very rare cases, the symptom may also occur on other situations.

Workaround: There is no workaround.

- CSCek71050

  Symptoms: Compared to other Cisco IOS software releases, unusually high CPU usage may occur in the BGP router process on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1.

  Conditions: This symptom is observed when BGP is learning routes from the RIB, even if redistribution is not directly configured under BGP. (Redistribution from other routing protocols to BGP can exacerbate the CPU usage.)

  Workaround: There is no workaround.

- CSCek76776

  Symptoms: The configuration of a deleted subinterface may show up on a new subinterface and may cause a traffic outage.

  Conditions: This symptom is observed on a Cisco router that has IP interface commands enabled when a script adds and deletes ATM subinterfaces on a regular basis.

  Workaround: Verify the subinterface configuration. When the configuration of a subinterface cannot be deleted, delete the subinterface, and then create a dummy subinterface that will pull the configuration that could not be deleted. Then recreate the first subinterface with a new configuration.

- CSCek77898

  Symptoms: A router that runs BGP may crash when paths are imported from the global table into a VRF via the **import** *address-family* **map** *route-map* command under a VRF.

  Conditions: This symptom is observed when the import is denied for a path that was previously allowed to be imported into the VRF and may occur, for example, after a configuration change for the import route map.

  Workaround: There is no workaround.

- CSCek78043

  Symptoms: A high CPU usage may occur in the BGP scanner process when an IP prefix is imported from the global table into a VRF table or when a topology is imported.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR when either the **import** *address-family* command is entered under a VRF or when the **import topology** *topology-name* command is entered under a BGP configuration.

Workaround: There is no workaround.

- CSCsd16043

  Symptoms: A Cisco IOS platform that is configured for Auto-RP in a multicast environment may periodically lose the RP to group mappings.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.3(17) when the RP drops the Auto-RP announce messages, which is shown in the output of the **debug ip pim auto-rp** command. This situation may cause a loss of multicast connectivity while the RP mappings are purged from the cache. See the following output example:

  ```
  Auto-RP(0): Received RP-announce, from ourselves (X.X.X.x), ignored
  ```

  Note that the symptom may also affect other releases.

  Workaround: Create a dummy loopback interface (do not use the configured IP address in the whole network) and use the **ip mtu** to configure the size of the MTU for the RP interface to 1500 and the size of the MTU for the dummy loopback interface to 570, as in the following examples:

  ```
  interface Loopback1
   ip address 10.10.10.10 255.255.255.255
   ip mtu 570
   ip pim sparse-mode
  end
  ```

  (This example assumes that the Auto-RP interface is loopback 0.)

  ```
  interface Loopback0
   ip address 10.255.1.1 255.255.255.255
   ip mtu 1500
   ip pim sparse-dense-mode
  end
  ```

- 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.

- CSCsf27220

  Symptoms: A router in which an ATM port adapter is installed may crash.

  Conditions: This symptom is observed on a Cisco router that is configured for Next Hop Resolution Protocol (NHRP) when traffic is sent.

  Workaround: There is no workaround.

- CSCsg16778

  Symptoms: A router may reload when Border Gateway Protocol (BGP) neighbor statements are removed from the configuration.

  Conditions: This symptom is observed in rare circumstances on a Cisco router when BGP neighbors are removed very quickly by a script at a much faster rate than manually possible and when a large BGP table is already present on the router before the script adds and removes the BGP neighbors.

  Workaround: There is no workaround.

  Further Problem Description: If you manually remove the BGP neighbors, it is less likely that the symptom occurs.

- 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.

- CSCsg90755

  Symptoms: When a Cisco router that has redundant RPs that function in RPR+ or SSO mode is reloaded, the standby RP may not boot correctly and may continuously reload.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that has an IPv4 MDT address family. The symptom occurs because of configuration synchronization issues that are related to the IPv4 MDT address family.

  Workaround: There is no workaround.

- 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.

- CSCsh24687

  Symptoms: After you have changed the default local preference, the bestpath recalculation does not occur for the BGP VPNv4 table.

  Conditions: This symptom is observed on a Cisco router when you enter the **clear ip bgp * vpnv4 unicast soft** command after you have changed the default local preference.

  Workaround: There is no workaround.

- 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.

- CSCsh66406

  Symptoms: When you enter the **maximum route** VRF configuration command or reduce the *limit* argument of the **maximum route** VRF configuration command, stale routes may occur in the BGP VPNv4 table.

Conditions: This symptom is observed on a Cisco router that functions as a PE router when the connection with a CE router is configured for another protocol than BGP such as OSPF and when the routes are redistributed into BGP.

Workaround: If OSPF is the other protocol, enter the **redistribute ospf** address family configuration command.

- CSCsh78277

  Symptoms: An "Mwheel" CPU hog condition may occur, and the platform may crash.

  Conditions: This symptom is observed in a multicast configuration when an RPF link changes.

  Workaround: There is no workaround.

- CSCsh79933

  Symptoms: A BFD session works correctly for an EIGRP neighbor but only until the first BFD failure event occurs. After the first failure event has occurred, BFD sessions are not re-established for any EIGRP neighbors over the interface on which the BFD failure event occurred. EIGRP neighbors are re-established and function correctly, however without the benefits of BFD. The symptom occurs on a per-interface basis. BFD sessions can be verified by entering the **show bfd neighbor** command.

  Symptoms: This symptom is observed in a basic configuration involving at least two routers that are connected through a link that is configured for EIGRP and BFD.

  Workaround: Restart EIGRP.

- CSCsh82953

  Symptoms: On a PE router in an EIGRP network, EIGRP prefixes are redistributed into BGP but are missing their EIGRP-derived extended community values.

  Conditions: This symptom is observed only when a **network** command is manually entered in "router EIGRP" mode while the **redistribute eigrp** command already exists in the BGP configuration. The symptom does not occur if all final configuration statements are present at router bootup time.

  Workaround: Re-enter the **redistribute eigrp** command in the BGP configuration. There is no need to first remove the command because entering the command triggers a new redistribution event.

- CSCsh86124

  Symptoms: A BGP neighbor that uses an IPv6 peer address may not be established, and the neighbor state may be idle.

  Conditions: This symptom is observed when the interface that connects to the peer flaps.

  Workaround: Enter the **neighbor** *ip-address* **shutdown** router configuration command followed by the **no neighbor** *ip-address* **shutdown** router configuration command.

- CSCsh96955

  Symptoms: The next hop for a BGP route is marked as "inaccessible," preventing the route from being advertised to peers or installed in the routing table.

  Conditions: This symptom is observed on a Cisco router when all of the following conditions are present:

  - The route is an IPv6 route with an IPv6 next hop.
  - The route is learned from an IPv6 eBGP router that is one hop away.

- Peering occurs between loopback addresses.
- The **disable-connected-check** command is configured for the peer from which the route is learned.

Workaround: Disable the **disable-connected-check** command on the peer from which the route is learned. Rather, configure eBGP multihop.

- CSCsi03359

  Symptoms: A PIM hello message may not reach the neighbor.

  Conditions: This symptom is observed on a Cisco router when an interface comes up and a PIM hello message is triggered.

  Workaround: Decrease the hello timer for PIM hello messages.

  Further Problem Description: The symptom occurs because the PIM hello message is sent before the port can actually forward IP packets. IGP manages to get its neighborship up but PIM does not, causing RPF to change to the new neighbor and causing blackholing to occur for up to 30 seconds.

- CSCsi06948

  Symptoms: A switch or router may crash because of a bus error after a BGP dampening-related command is entered.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch that has a Supervisor Engine 720 that runs Cisco IOS Release 12.2(18)SXF7 but may also affect other platforms and releases.

  Workaround: There is no workaround.

- CSCsi42566

  Symptoms: A router may crash when the you enter the **show bgp l2vpn vpls rd** *vpn-rd* command.

  Conditions: This symptom is observed on a Cisco router when BGP is configured but an L2 VPN address family is not configured.

  Workaround: When the router does not have an L2 VPN address family, do not enter the **show bgp l2vpn vpls rd** *vpn-rd* command.

- 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.

- CSCsi82425

  Symptoms: When a secondary IP address is removed from an interface, the entire ARP table may be flushed.

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

  Workaround: There is no workaround.

- CSCsi84089

  Symptoms: A few seconds after OSPF adjacencies come up, a router crashes because of a bus error.

  Conditions: This symptom is observed on a Cisco router that functions as an ISR that is configured for OSPF.

Workaround: Add area 0 in the OSPF VRF processes.

Alternate Workaround: Enter the **no capability transit** command in the OSPF VRF processes.

- CSCsi86386

  Symptoms: The **clear ip bgp * soft in** command does not function for an inbound route map.

  Conditions: This symptom is observed on a Cisco router that has the **neighbor send-label** command enabled when the prefix that is being filtered is an IPv4 unicast prefix.

  Workaround: Enter the **clear ip bgp *** command.

  Further Problem Description: The **clear ip bgp * soft in** command does function fine for other address families such as VRF and VPNv4.

- CSCsi97315

  Symptoms: When you remove the **neighbor** *peer-group-name* **fall-over bfd** command for a peer group, the configuration is not removed from the members of the peer group, and the members may still register with through Bidirectional Forwarding Detection (BFD).

  Conditions: This symptom is observed on a Cisco router that has the following configuration:

  ```
  router bgp <as-number>
  neighbor <peer-group-name> peer-group
  neighbor <peer-group-name> remote-as <as-number>
  neighbor <peer-group-name> fall-over bfd
  neighbor <ip-address> peer-group <peer-group-name>
  ```

  When you enter the **neighbor** *peer-group-name* **fall-over bfd** command, the IP address that is associated with this command is not removed.

  Workaround: Remove and reconfigure the neighbor.

- CSCsj17820

  Symptoms: A router may crash when an MGRE tunnel interface that is configured for NHRP is removed.

  Conditions: This symptom is observed on a Cisco router that functions in a DMVPN network and occur only when the tunnel interface is removed through an automated script. The symptom does not occur during manual removal of the tunnel interface.

  Workaround: There is no workaround.

- 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.

- CSCsj25940

  Symptoms: A router that is configured for EIGRP and BFD may generate the following error message and traceback:

  ```
  %SYS-2-NOTQ: unqueue didn't find 667BD8F4 in queue 644087B4
  -Process= "Exec", ipl= 0, pid= 3,
  -Traceback= 0x608452B4 0x609CBCDC 0x612D8128
  ```

Conditions: This symptom is observed on a Cisco router after you have entered the following commands:

```
Router(config)#router eigrp <as-number>
Router(config-router)#bfd interface <type number>
Router(config-router)#no bfd interface <type number>
```

Workaround: There is no workaround.

- CSCsj61743

  Symptoms: A BGP neighbor may not be able to establish a session, causing the session to become stuck in the passive connect state on one side and in the idle state on the other side. When this situation occurs, the output of the **show ip bgp vpnv4 all neighbor** *neighbor-address* command shows the following:

```
BGP neighbor is <ADDRESS>,  vrf <VRF-name>,  remote AS <AS>, external link
...
  BGP state = Idle
...
  Neighbor sessions:
    0 active, is multisession capable
  Message statistics, flags passive, state Connect:
...
```

  Conditions: This symptom is observed on a Cisco router that functions in a large BGP configuration with many VRFs after an interface has flapped.

  Workaround: Enter **clear ip bgp *** command.

- CSCsj71306

  Symptoms: After an RP switchover has occurred, BGP does not send a new BGP MDT update. Because of this situation, the MDT tunnel interface does not come up, and all multicast data traffic between VRFs is dropped after another RP switchover has occurred.

  Conditions: This symptom is observed after an RP switchover has occurred on a Cisco router that is configured for MVPN and that functions in SSO mode.

  Workaround: Enter the **clear ip bgp *** command.

- CSCsj89029

  Symptoms: A router may crash after you have removed the route distinguisher (RD) for a VRF.

  Conditions: This symptom is observed when the VRF from which the RD was removed includes prefixes that were learned via BGP and that were imported from the global table.

  Workaround: There is no workaround.

- CSCsk19583

  Symptoms: A Multicast Virtual Private Networks (MVPN) may not function.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1, that uses extended communities to communicate the MDT information, and that interoperates with a Cisco IOS release that is earlier than Release 12.0(29)S or Release 12.2(31)SB.

  Workaround: There is no workaround.

- CSCsk39804

  Symptoms: The multicast Connection Admission Control (CAC) state may be incorrect after multicast routes have been cleared.

Conditions: This symptom is observed on a Cisco router that has Source Specific Multicast (SSM)-mapped channels that are locally joined on the router.

Workaround: There is no workaround.

- CSCsk43926

  Symptoms: High CPU usage may occur interrupt context on an RP, and spurious memory accesses may be generated when a route-map update is checked. You can verify this situation in the output of the **show align** command.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for BGP.

  Workaround: There is no workaround.

ISO CLNS

- CSCek76093

  Symptoms: A CLNS neighbor may still be formed after the IS-IS protocol has been shut down.

  Conditions: This symptom is observed only on serial interfaces.

  Workaround: There is no workaround.

- 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.

- CSCsh63785

  Symptoms: A MPLS tunnel may not come up after a stateful switchover (SSO) has occurred.

  Conditions: This symptom is observed on a Cisco router when Cisco IS-IS NSF is enabled and when IS-IS is used as the IGP for MPLS TE tunnels.

  Workaround: Do not configure Cisco IS-IS NSF. Rather, configure IETF NSF.

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

  Second Alternate Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that is used for the MPLS TE tunnels after the SSO has occurred.

- CSCsi41944

  Symptoms: After redistribution-related configuration changes have been made, a CPUHOG condition may occur in the Virtual Exec process, causing loss of IS-IS adjacencies.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch that runs Cisco IOS Release 12.2(18)SXF when the **redistribute maximum-prefix** command is configured under the **router isis** command and when BGP is configured to be redistributed into IS-IS. The symptom could also affect a Cisco 7600 series router that runs Release 12.2SR.

  Workaround: There is no workaround.

- CSCsi57971

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

- CSCsj53361

  Symptoms: IS-IS adjacencies may flap after a stateful switchover (SSO) has occurred.

  Conditions: This symptom is observed when there are large number of adjacencies (for example, 16) and when the IS-IS database is large (for example, one LSP containing 5000 routes).

  Workaround: Increase the hold time that is advertised in the IS-IS Hello (IIH) packet by entering the **router isis nsf advertise holdtime 90** command on the router on which the SSO occurs.

- 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.

- CSCsj83306

  Symptoms: IS-IS prefixes may be missing from the IP routing table and LDP peers may not come up after you have entered the **issu runversion** command.

  Conditions: This symptom is observed on a Cisco 7600 series that has the **nsf cisco** command configured for IS-IS.

  Workaround: Do not configure NSF for IS-IS.

- CSCsk47890

  Symptoms: A router may crash when you enter the **show isis database detail** command.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB on powerPC based platform such as an RSP720.

  Workaround: There is no workaround.

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
  0000000001111111111222222222333^ 12345678901234567890123456789012| | PROBLEM
  (Variable Overflowed).
  ```

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

- 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.

- CSCec24846

  Symptoms: System accounting is not sent as the first record when sessions are establishing while the system is coming up.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1.

  Workaround: There is no workaround.

- CSCek66092

  Symptoms: An IPv6 demultiplexer configuration is rejected over an Ethernet interface when there is an IP address configured on the same interface.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(33)SRB or a release later than Release 12.2(31)SB and that is configured for Xconnect.

  Workaround: There is no workaround.

  Further Problem Description: The following example shows a configuration in which the symptom occurs:

```
router(config)#interface FastEthernet5/0
router(config-if)#ip address 10.10.10.10 255.255.255.0
router(config-if)#xconnect 192.168.200.200 100 pw-class ipv6_demux
Incompatible with ip address command on Fa5/0 - command rejected.
```

- 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.

- CSCek68890

  Symptoms: Multicast traffic stops on one blade after both blades in a Blade-to-Blade stateful failover configuration are reloaded simultaneously.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when some interfaces are assigned to one IPSec VPN SPA and other interfaces to a second IPSec VPN SPA. The symptom occurs in the following scenario:

  – You reload the first blade.

  – You remove the second blade before the first blade comes back up so that both crypto engines are inactive for some time and all tunnels go down.

  After both crypto engines come back up and all SAs are re-established, multicast traffic only passes through the tunnels that are assigned to the first blade.

  The symptom does not occur when you reload one blade after the other, that is, when you wait until one blade comes back up before you reload the second blade.

  Workaround: To restore proper operation, enter the **hw-module subslot** *slot/subslot* **reload** command.

  Alternate Workaround: To restore proper operation, remove and re-add the tunnel configuration.

- CSCek69576

  Symptoms: The standby Route Switch Processor 720 (RSP720) may become stuck when it reloads after a switchover has occurred. Eventually, the RSP720 resets and boots fine thereafter. When the symptom occurs, the following error messages are generated:

  ```
  %ONLINE-SP-6-TIMER: Module 8, Proc. 0. Failed to bring online because of timer event
  %PFREDUN-SP-6-ACTIVE: Standby processor removed or reloaded, changing to Simplex
  mode)
  ```

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

  Workaround: There is no workaround.

- CSCek71534

  Symptoms: A SIP-600 crashes when sending H-VPLS traffic.

  Conditions: This symptom is observed on a Cisco 7600 series when the DA MAC address is in the range from 00.00.00.00.00.00 to 00.00.00.00.00.0F, when a 64-byte packet is sent encapsulated under VPLS, and when CFM continuity check is not configured on the interface of the SIP-600.

  The symptom occurs because CFM is zero but the DA MAC addresses in the range from 00.00.00.00.00.00 to 00.00.00.00.00.0F match the (unconfigured) CFM continuity check.

  Workaround: Enable CFM on the interface of the SIP-600 by entering the **ethernet cfm enable** global configuration command.

- CSCek71816

  Symptoms: An end-to-end ping fails when an ASBR restores a VRF in a multipath configuration with different autonomous systems.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB that functions in an EBGP VPNv4 multipath configuration.

Workaround: There is no workaround.

- CSCek74024

  Symptoms: A router that is configured for AAA may crash because of a bus error and generate the following error message:

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

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB or Release 12.2SRB and that has AAA authentication enabled.

  Workaround: There is no workaround.

- CSCek74480

  Symptoms: A router may not receive LDP traps that use SNMP VRF-aware context.

  Conditions: This symptom is observed when SNMP context is associated with a particular VRF and when LDP traps are enabled to use the SNMP context.

  Workaround: Check the syslog messages on the router and not rely on LDP traps.

- CSCek75082

  Symptoms: A router may crash when you unconfigure a T3 controller.

  Conditions: This symptom is observed in the following topology on a Cisco router (router B) when you unconfigure a channel group on another router (router A) while traffic is being processed:

  ```
  Traffic generator<------->router A<-------->router B<------->Traffic generator
  ```

  In this situation, router B crashes. The following sequence of commands on the routers causes router B to crash:

  ```
  router A#conf t
  Enter configuration commands, one per line.  End with CNTL/Z.
  router A(config)#controller T3 7/0
  router A(config-controller)#no t1 1 channel-group 0 timeslots 1-24
  ```

  ```
  router B#conf t
  Enter configuration commands, one per line.  End with CNTL/Z.
  router B(config)#controller T3 7/0
  router B(config-controller)#no t1 1 channel-group 0 timeslots 1-24
  ```

  Workaround: There is no workaround.

- CSCek76105

  Symptoms: When IPv6 multicast traffic is forwarded, the following type of alignment tracebacks may be generated:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at [memory address] reading 0x34
  %ALIGN-3-TRACE: -Traceback= [stack trace]
  ```

  Conditions: This symptom is observed when a tunnel that carries IPv6 multicast traffic is deleted.

  Workaround: There is no workaround.

- CSCek76878

  Symptoms: In a VRF that is configured for CsC and that uses LDP as the label distribution protocol between a PE and CE router, end-to-end MPLS connectivity breaks after an SSO switchover occurs for the Route Processors. After the switchover has occurred, the PE router fails to reallocate the local MPLS labels for the remote prefixes, preventing LDP from re-advertising the local MPLS labels to the CE routers.

  Conditions: This symptom is observed on a PE router that runs a Cisco IOS software image that integrates the fix for caveat CSCse67910 when all PE routers in the MPLS VPN network are configured with the same Route Distinguisher (RD) for the VRF. A list of the affected releases can

be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse67910. Cisco IOS software releases that are not listed in the "First Fixed-in Version" field at this location are not affected.

For the Cisco 7600 series, the symptom may occur in Release 12.2(33)SRB and Release 12.2(33)SRB1.

Workaround: Do not use LDP label distribution between the PE and CE routers. Rather, use BGP.

First Alternate Workaround: For the VRF, use different RDs on the PE routers in the MPLS VPN network.

Second Alternate Workaround: Enter the **clear ip route vrf** *vrf-name* * command for the VRF.

- CSCek78653

  Symptoms: A Point-to-Point Tunneling Protocol (PPTP) session may not be established, and the following error message may be generated:

  ```
  SSS MGR [uid:4]: ERROR - Failed to initialize FM Segment. Could not start Local service
  ```

  Conditions: This symptom is observed on a Cisco router that functions as an LNS and that terminates PPTP sessions that have ISG features applied to them.

  Workaround: Disable the ISG features. If this is not an option, there is no workaround.

- CSCek79390

  Symptoms: Egress traffic may not be forwarded when Traffic Engineering/Fast Reroute (TE-FRR) is configured on the same grouping of 10x1GE ports on an Ethernet Services (ES20) line card or on a SIP-600.

  Conditions: This symptom is observed on a Cisco 7600 series when the protected tunnel and backup tunnel reside on the same data path on the ES20 line card or on the same SIP-600.

  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.

- 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.

- 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.

- 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.

- CSCsb85030

  Symptoms: Packets such as DHCP packets may be dropped, and MAC addresses may not be learned on interfaces even though the interfaces are in the up/up state.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when you first configure and then remove port security.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, manually configure the MAC addresses in the MAC-address table.

  Alternate Workaround: Re-enable and then disable port security once more on the affected ports.

- CSCsc32189

  Symptoms: ISAKMP does not check multiple transform payloads in one proposal, preventing a particular third-party vendor L2TP/IPSec client from using the ESP-3DES-SHA transform set.

Conditions: This symptom is observed when the particular third-party vendor L2TP/IPSec client sends the following proposal and when the Cisco IOS software checks only the first transform set and not the second one.

```
Proposal payload # 1
   Next payload: Proposal (2)
   Length: 92
   Proposal number: 1
   Protocol ID: IPSEC_ESP (3)
   SPI size: 4
   Number of transforms: 2
   SPI: 58CB6150
   Transform payload # 1
      Next payload: Transform (3)
      Length: 40
      Transform number: 1
      Transform ID: 3DES (3)
      SA-Life-Type (1): Seconds (1)
      SA-Life-Duration (2): Duration-Value (3600)
      SA-Life-Type (1): Kilobytes (2)
      SA-Life-Duration (2): Duration-Value (250000)
      Encapsulation-Mode (4): Transport (2)
      Authentication-Algorithm (5): HMAC-MD5 (1)
   Transform payload # 2
      Next payload: NONE (0)
      Length: 40
      Transform number: 2
      Transform ID: 3DES (3)
      SA-Life-Type (1): Seconds (1)
      SA-Life-Duration (2): Duration-Value (3600)
      SA-Life-Type (1): Kilobytes (2)
      SA-Life-Duration (2): Duration-Value (250000)
      Encapsulation-Mode (4): Transport (2)
      Authentication-Algorithm (5): HMAC-SHA (2)
```

Workaround: Do not use the ESP-3DES-SHA transform set. Rather, use the ESP-3DES-MD5 transform set.

- CSCsc59025

  Symptoms: The **udld port disable** command may be missing for an interface after several HA switchovers have occurred, causing UniDirectional Link Detection (UDLD) to be enabled on the interface.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router when UDLD is globally enabled but disabled on the interface for which you entered the **udld port disable** command.

  Workaround: There is no workaround. Note that UDLD is disabled by default. When you enter the **udld port disable** command for an interface, you configure “no configuration of UD.”

Further Problem Description: When you configure the **udld port aggressive** command globally, then enter the **udld port disable** command for an individual port, and then the symptom occurs, the **udld port aggressive** command remains enabled on the individual port. A workaround for this situation is to enter the **no udld port aggressive** command on the individual port.

- 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.

- 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
```

- CSCsd65434

  Symptoms: After a router has received an IGMP leave message for a group on a switchport and a user is still connected to this group while an IGMP general query is sent on the same interface, the group is cleared either immediately or after 10 seconds, and then added again when a join message is received.

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

  Workaround: Configure the DSLAM ports as IGMP snooping ports in a static multicast router configuration by entering the **ip igmp snooping mrouter interface** *type slot/port* command.

  Alternate Workaround: Add the multicast MAC address statically by entering the **mac-address-table static** *mac-addr* **vlan** *vlan-id* **interface** *type slot/port* command.

- 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.

- 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.

- 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.

- CSCse95996

  Symptoms: A configlet that is presented to a router via CNS configuration agents or via a NETCONF session may fail.

  Conditions: This symptom is observed with both syntax check turned on and syntax check turned off.

  Workaround: Use the action-on-fail=”continue” attribute when using CNS configuration agents or a NETCONF session.

- CSCsf18752

  Symptoms: GTP SLB does not function. GPRS PDP context create requests are forwarded to the GGSN, but they all go to a singe GGSN instead of being load-balanced over several GGSNs, and GTP IMSI sticky delete notifications are not created. In addition, when GTP SLB-related debugs are enabled, no debug messages are printed.

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA5 when both the following conditions are met:

- The **mls ip slb search wildcard rp** is configured on the supervisor engine that functions as an SLB.
- More than one pair of GTP SLB server farms and vservers are configured.

Workaround: Remove **mls ip slb search wildcard rp** command from the supervisor engine.

- 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.

- CSCsg07525

  Symptoms: Packet loss may occur every 30 seconds over a distributed port channel on a Distributed Forwarding Card (DFC) card because the "TestScratchRegister" that runs every 30 seconds disrupts the normal RAN Backhaul (RBH) calculation.

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

  Workaround: Disable the "TestScratchRegister" on the affected DFC by entering the following diagnostic command:

  Router(config)# no diagnostic monitor module <mod#> test TestScratchRegister

- 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.

- CSCsg16272

  Symptoms: When you perform an OIR for a WS-6748-GE-TX or WS-6724-SFP, the module does not generate a linkDown SNMP trap for a physical wire that is connected to the port.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router. Note that the symptom does not occur for a WS-6704-10GE.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, look into the syslog to find the "%LINK-3UPDOWN" message for the port.

- 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.

- 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.

- 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.

- CSCsg79129

  Symptoms: Multicast traffic may not be forwarded on a routed VPLS (R-VPLS) interface that is configured for PIM Sparse Mode (SM).

  Conditions: This symptom is observed on a Cisco 7600 series that has a SIP-600 on which an RPF interface is configured and occur when egress replication mode is enabled.

  Workaround: Change the multicast replication mode from egress mode to ingress mode by entering the **mls ip multicast replication-mode ingress** command.

- 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.

- CSCsg98728

  Symptoms: A ping from one CE router to another CE router through an AToM tunnel does not go through properly.

  Conditions: This symptom is observed on a Cisco router when the AToM tunnel runs over two different autonomous systems.

  Workaround: There is no workaround.

- CSCsh22171

  Symptoms: After an MPLS-TE path is rerouted, the Virtual Private LAN Services (VPLS) feature stops decapsulating Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) frames that are received from a remote PE router. This situation may result in an STP loop.

  Conditions: This symptom is observed on a Cisco 7600 series that functions as a PE router in an MPLS network, that has many MPLS-TE tunnels configured, and that has the **l2protocol-tunnel stp** command enabled.

  Workaround: Enter the **no l2protocol-tunnel stp** command.

- CSCsh23176

  Symptoms: A router crashes when you unconfigure RIP.

  Conditions: This symptom is observed on a Cisco router and is more likely to occur when there are many RIP routes configured.

  Workaround: Remove all network statements that are defined under the **router rip** command, wait for all RIP routes to age-out, then remove the **router rip** command.

- CSCsh24450

  Symptoms: A memory leak may occur when tunnels or sessions are created and deleted in quick succession.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.2SRB, or Release 12.2SXH and that is configured for SNMP.

  Workaround: If a virtual template is used, enter the **no virtual-template snmp** command to prevent the symptom from occurring. If no virtual template is used, there is no workaround.

- CSCsh25976

  Symptoms: There are two symptoms:

  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. 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.

- CSCsh27931

  Symptoms: A platform may crash when an arithmetic exception crash occurs. Before this situation occurs, the following error message is generated:

  ```
  %COMMON_FIB-SP-4-UNEQUAL: Ratio of unequal path weightings (1 1 40) prevents oce IP
  adj out of GigabitEthernet3/2, <ip addr> from being used.
  ```

  Conditions: This symptom is observed on a Cisco platform that functions in an IS-IS configuration when TE tunnels are shut down.

  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. A bad SFP means an incompatible/unsupported/faulty SFP.

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

- CSCsh30617

  Symptoms: A Cisco router may unexpectedly reload when the Embedded Event Manager (EEM) applet is removed from the configuration or shortly after the EEM applet has been removed.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(10.8)T or a later release and occurs most often when the applet was registered when the router booted. The symptom is not release-specific.

  Workaround: There is no workaround.

- CSCsh33128

  Symptoms: A VRF may not be created correctly. When this situation occurs, associated internal VLANs are not allocated. As a result, when a partial shortcut is installed, the internal partial VLAN is not included in the outgoing interface list (olist).

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router only when VRFs are added in a clean configuration and when hardware switching is enabled.

  Workaround: Disable and re-enable hardware switching.

- CSCsh41459

  Symptoms: A router crashes when you remove and then add back VRFs.

  Conditions: This symptom is observed on a Cisco router that functions as a PE Router in an MPLS VPN network.

  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.

- CSCsh54380

  Symptoms: On SIP600/ESM20G line cards that are running VPLS/EoMPLS in a highly scaled configuration, stats may be inaccurate when traffic engineering tunnels are configured with Fast Reroute and a failover scenario is encountered.

  Conditions: When a large number of VPLS VCs are configured and if all of these VCs are protected by FRR and traffic is failed over between protected and backup interfaces, the line card may experience a stats problem where the VCs may not be able to account the stats accurately.

  This problem is seen in the following configuration scenarios:

  When one of the traffic engineering tunnel's primary or backup interface is configured on:

  ```
  A port on a SIP-600 or
  A port from 0..19 on  a ESM20G(20x1GE) or
  First port (port 0) of a ESM20G (2x10GE)
  ```

and the other tunnel's interface is configured on:

```
Any port from 10-19 of ESM20G 20x1GE or
Second Port (port 1) of ESM20G 2x10GE
```

Workaround: There is no workaround.

- 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.

- CSCsh64335

  Symptoms: A router may crash when you enter the **mkdir** command to create a directory with a length of more than 127 characters and when you query this directory via SNMP.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system.

  Workaround: There is no workaround.

- CSCsh69420

  Symptoms: Connected routes that are redistributed via IPv6 VPN over MPLS (6VPE) into a VRF in an IPv6 address family for BGP may not be subsequently imported into another VRF.

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

  Workaround: There is no workaround.

- CSCsh70638

  Symptoms: When a router boots and when bursty traffic occurs, the following error messages may be generated:

  ```
  %ALIGN-SP-STDBY-3-SPURIOUS: Spurious memory access made at 0x72AB2370 reading 0xB8
  %ALIGN-SP-STDBY-3-TRACE_SO:
  -Traceback= (s72033-adventerprisek9_wan_dbg-0-dso-bn.so+0x1AE370) ([42:0]+0x1AE47C)
  ([31:-3]3-dso-b+0x220994) ([41:0]+0x220FB8) ([41:0]+0x221A90) ([41:0]+0x22214C)
  ([41:0] +0x222D6C) ([41:0]+0x2233CC)
  ```

  Conditions: This symptom is observed when bursty IPC traffic occurs while the router boots or during a switchover, typically with heavy configuration data exchanges.

  Workaround: There is no workaround.

- CSCsh72267

  Symptoms: A PVC that is configured on an ATM interface that is configured for cell packing may not receive the MNCP and MCPT parameters from the ATM interface. (MNCP = Maximum cells packed in one MPLS packet; MCPT = Maximum time to wait to pack the cells in one MPLS packet.)

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

Workaround: Do not configure cell packing on the ATM interface. Rather, configure cell packing directly on the PVC.

- CSCsh79194

  Symptoms: Unexpected HSRP debug messages such as the following one may be generated when only a partial debug has been enabled:

  ```
  HSRP: Et0/0 Grp 1 Active: l/Hello rcvd from lower pri Standby router (110/10.0.0.102)
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for HSRP when the **debug** *standby terse* command is enabled.

  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.

- 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.

- CSCsh97826

  Symptoms: VPNv6 forwarding entries may not be properly installed on an VPNv6 ASBR, and the following error message may be generated:

  ```
  %BGP_MPLS-3-VPN_REWRITE: installing rewrite for [100:2]CC:5::/32 failed: Illegal
  parameter
  ```

  Conditions: This symptom is observed on a Cisco router that functions as an ASBR that has IPv6 enabled on the interface that connects to a remote ASBR when this remote ASBR does not have IPv6 enabled on the peering interface.

  Workaround: Configure the peering interfaces consistently on both ASBRs. Either both ASBRs should have IPv6 enabled, or both ASBRs should have IPv6 disabled on the peering interfaces.

- CSCsh98208

  Symptoms: PIM Snooping causes duplicate multicast packets to be delivered in the network.

  Conditions: This symptom is observed when the shared tree and SPT diverge in a VLAN on a Cisco Catalyst 6500 series switch or Cisco 7600 series router that have PIM Snooping configured. PIM Snooping may suppress the (S,G) RPT-bit prune message that is sent by the receiver from reaching the upstream router in the shared tree, causing a situation in which more than one upstream router forward the multicast traffic by using their respective (S,G)-join state, and, in turn, causing duplicate multicast packet to be delivered to the receivers. This situation lasts only for a brief moment because the PIM-ASSERT mechanism kicks in and stop the extraneous flow. However, this cycle repeats again when the next (*,G) join (S,G) RPT bit prune message is sent by one of the receivers.

  Workaround: Disable PIM Snooping in the VLAN-interface configuration.

  Alternate Workaround: If the command is available in the release that you are running, enter the **no ip pim snooping suppress sgr-prune** command to disable SGR-prune message suppression.

- CSCsh98953

  Symptoms: When a PE router that is configured for L2TPv3 receives a Start-Control-Connection-Request (SCCRQ) message from a peer PE router and is unable to locate authorization information for this peer PE router, the PE router may respond with a S top-Control-Connection-Notification (StopCCN) message, and a memory leak may occur.

  Conditions: This symptom is observed when there is a misconfiguration or when the peer PE router sends the SCCRQ message before you have finished entering the Xconnect configuration on the PE router.

  Workaround: There is no workaround.

- CSCsi11257

  Symptoms: After an SSO switchover has occurred, the following error message is generated on the newly active supervisor engine:

  ```
  %SFF8472-3-READ_ERROR: Gi3/24: Error reading DOM data from transceiver
  ```

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

  Workaround: There is no workaround. However, note that the error message is false and can be ignored.

- CSCsi29423

  Symptoms: A ping may not go through an Ethernet Services (ES20) line card when packet verification is enabled.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when packets are corrupted at the tail part.

  Workaround: There is no workaround.

- CSCsi32655

  Symptoms: The running configuration of a Content Switching Module may be unexpectedly cleared. The CSM still appears to work fine, but the configuration cannot be accessed, edited, or updated.

  Conditions: This symptom is observed on a Cisco 6500 series switch and Cisco 7600 series router when you enter the **module csg** *slot-number* command in which the *slot-number* argument represents the module number of a configured CSM.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reboot the platform without saving the configuration to restore the running configuration.

- CSCsi40628

  Symptoms: A Cisco Group Management Protocol (CGMP) packet that is caught by Remote SPAN (RSPAN) may end up in a Layer 2 loop, being sent back and forth continuously between two platforms. When this situation occurs, the CPU usage on the supervisor engine may become very high, and a spanning tree loop may occur.

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

  - There are at least two RSPAN VLANS configured (for example, VLAN x and VLAN y).
  - The RSPAN source for one RSPAN VLAN (VLAN x) is on a different platform than the RSPAN source for the other RPSAN VLAN (VLAN y).
  - One of the platforms on which an RSPAN VLAN source is configured receives a CGMP packet.

  Workaround: Configure a monitor filter to enable all VLANs except RSPAN VLANs. For example, if the RSPAN VLANs are VLAN 600 and VLAN 601, configure the following:

  ```
  monitor session 1 filter vlan 1 - 599 , 602 - 4094
  ```

  First Alternate Workaround: Remove the SPAN source from one of the two platforms.

  Second Alternate Workaround: Remove the CGMP configuration.

- 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.

- CSCsi42517

  Symptoms: A Cisco 7600 series may crash when Cisco IOS-SLB receives a GSN backup update packet.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in an HSRP configuration and that has virtual servers configured when none of the virtual servers has the **service gtp-inspect** command enabled.

  Workaround: There is no workaround because the situation that is described in the Conditions is a misconfiguration.

- CSCsi45840

  Symptoms: ARP requests to an HSRP virtual IP address may fail.

  Conditions: This symptom is observed when the same HSRP IP address is used alternatively on different interfaces, and when one of these interfaces has the **switchport** command configured and unconfigured several times.

  Workaround: Remove the HSRP configuration from the interface before you enter the **switchport** command on the interface.

- CSCsi46861

  Symptoms: The RP of a Cisco 7600 series that is configured for MPLS may generate the following error message and traceback:

  ```
  %MFI-3-REDISTMGR: Redistribution Manager: stats_updates - not in use 3
  - Traceback= 406298C4 40629E08 428DEA78 40F3D13C 4180B62C 418083C0 41E91C18 426C61E0
  41E9D140 40A475B4 419E032C 419E0758 4155B838 4155B824
  ```

  Conditions: This symptom is observed rarely after a switchover has occurred.

  Workaround: There is no workaround. However, the functionality of the router is not impacted.

- 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.

- CSCsi49953

  Symptoms: One of the CPUs of a SIP-200 may crash continuously when an LFI bundle is present on the SIP-200.

  Conditions: This symptom is observed on Cisco 7600 series routers that are connected back-to-back when no traffic is processed.

  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.

- CSCsi53644

  Symptoms: After an SSO switchover has occurred, when the standby RP enters the hot standby mode, an MLS CEF entry may be missing for a loopback interface on the newly active RP. The RP that was the active RP before the SSO switchover occurred and that is now the RP in the hot standby mode still has the correct MLS CEF entry.

  Conditions: This symptom is observed on a Cisco router when you enter the **redundancy force-switchover** to initiate an SSO switchover.

  Workaround: For the loopback interface that does not have the MLS CEF entry on the newly active RP, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command to repopulate the MLS CEF entry.

- CSCsi56504

  Symptoms: The output of the **show atm pvc** command does not show proper QoS values. Even when QoS is configured for VBR or ABR, the command output always shows UBR.

  Conditions: This symptom is observed on a Cisco router that is configured with a PVC bundle.

  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.

- 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.

- CSCsi65363

  Symptoms: When you attempt to bring up a T1 link on a PA-MC-2T3 port adapter, the serial interface may remain in up/down state. In this situation, Layer 1 is fine.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that have a FlexWAN in which a PA-MC-2T3 port adapter is installed when PPP, HDCL, or Frame Relay encapsulation is used on the serial interface.

  Workaround: Move the T1 link to another slot of the PA-MC-2T3 port adapter or move the PA-MC-2T3 port adapter to another slot of the FlexWAN. Also, when you tear down the T1 channel-group configuration and reconfigure, the symptom may disappear.

  Further Problem Description: Note that when you configure a local loopback interface on the controller of the T1 (or T3) interface and configure HDLC encapsulation on the serial interface, you can bring up the serial interface.

- CSCsi65916

  Symptoms: A large I/O memory leak may occur on a Supervisor Engine 720 that functions in a Cisco Mobile Exchange environment.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when MWAM or SAMI processors are configured for remote logging and when many system messages from the MWAM or SAMI processors are directed to the supervisor engine.

  Workaround: There is no workaround.

- 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.

- CSCsi70356

  Symptoms: You may enter an image name length (including the prefix) of greater than or equal to 64 characters but less than the prefix length plus 64 characters in the **issu loadversion** *active-slot active-image standby-slot standby-image* command. The router should prevent ISSU from occurring in this situation, but it does not. As a result, the standby RP is reloaded but does not enter SSO mode, causing the ISSU software upgrade to fail.

Conditions: This symptom is observed only when Cisco IOS software image is renamed on the file system in such a way that the image name (including the prefix) is larger than or equal to 64 characters but less than the prefix length plus 64 characters.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **write memory** command followed by the **redundancy reload peer** command to recover the standby RP.

- CSCsi72323

  Symptoms: The 10-Mbps and 100-Mbps links of a 20-port Ethernet Services line card (7600-ES20-GE) may go down.

  Conditions: This symptom is observed on a Cisco 7600 series after you have reloaded the platform while diagnostics are enabled. Ports with a copper SFP that are configured for 10-Mbps and 100-Mbps go down after the platform boots. The symptom does not occur when diagnostics are disabled.

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

- CSCsi74605

  Symptoms: The state of VPLS VCs on a Virtual Forwarding Instance (VFI) may remain up even though the state of the interface VLAN is down, which can be seen in the output of the **show mpls l2transport vc** command. In this situation, there is no corresponding L2 circuit in the up state, which can be seen in the output of the **show interface vlan** command.

  Conditions: This symptom is observed an a Cisco 7600 series that has the **xconnect vfi** command configured for VPLS services under an interface VLAN.

  Workaround: There is no workaround to prevent the symptom from occurring. You must ensure that the VPLS VCs and the interface VLAN are in the up state so that traffic can flow.

- 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.

- CSCsi91324

  Symptoms: Immediately after an interface in the outgoing interface list (OIL) goes down, a brief period of packet loss to interfaces in the OIL may occur. During this brief period, the Multicast MultiLayer Switching (MMLS) hardware entry on the Distributed Forwarding Card (DFC) is deleted and re-installed.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB in the following configuration:

  - Source Specific Multicast (SSM) is enabled.
  - IGMP Snooping is disabled.
  - A static join is configured on the interfaces.
  - The **mls ip multicast consistency-check** command is enabled.

  Workaround: Disable the **mls ip multicast consistency-check** command.

Further Problem Description: When the **mls ip multicast consistency-check** command is enabled, a linkdown event is detected ahead of multicast route updates, and the inconsistency is corrected. This situation results in a hardware entry reset.

- CSCsi93683

  Symptoms: In Cisco IOS software that is running the Bidirectional Forwarding Detection (BFD) protocol, attempts to remove BFD sessions may fail.

  Conditions: The symptom has been observed after the maximum number of supported sessions has been configured. The maximum number is 128 in most but not all releases.

  Workaround: There is no workaround.

- CSCsi95192

  Symptoms: When a Cisco 7600 series crashes, the crashinfo file that is collected may not be complete, affecting the debug information.

  Conditions: This symptom is observed on a Cisco 7600 that has a Route Switch Processor 720 (RSP 720).

  Workaround: Configure a larger crashinfo file size for the RSP 720, as in the following example:

  ```
  exception crashinfo buffersize 80
  ```

- CSCsi96685

  Symptoms: A router that functions as an LNS and ISG may crash at the “chunk free” function when a call is being freed or disconnected.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB and is caused by a race condition. The symptom may not be release-specific.

  Workaround: There is no workaround.

  Further Problem Description: The following configuration suggestions may reduce the likelihood that the race condition occurs:

  - Change the following in all VPDN groups:

    ```
    l2tp tunnel receive-window 10000
    l2tp tunnel timeout hello 180
    ```

  - Do not configure the router for SSO. Rather, configure RPR+.
  - If the following command is not required, remove it from the configuration:

    ```
    aaa authentication ppp user-auth if-needed group csm-auth-acct
    ```

  - Configure the *seconds* argument of the **radius-server timeout** *seconds* command to 5 seconds.
  - Configure the *tries* argument of the **radius-server dead-criteria tries** *tries* command to its maximum value. (If there is only one RADIUS server, you need to ensure that it is not going to be marked dead.)
  - Periodic accounting every 90 minutes may be too aggressive and may need to be changed.
  - Set the *time-limit* argument of the **ppp timeout ncp** *time-limit* command under the virtual template to 45 seconds.

- 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.

- CSCsi99825

  Symptoms: An SNMP Engine may crash at the “idb_get_swsb” and “mpls_if_get_gen_stats” functions.

  Conditions: This symptom is observed on a Cisco 7613 that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: Disable this SNMP query from the CU.

- CSCsj00449

  Symptoms: An output queuing policy may be rejected by an EFP on an Ethernet Services (ES20) line card when the LLQ policer rate in the policy is more than 1 Gbps, and a warning message is generated that states that rates greater than 1 Gbps are not supported. However, a much higher policer rate is supported.

  Conditions: This symptom is observed on a Cisco 7600 series when you apply a relevant service policy to a service instance.

  Workaround: There is no workaround.

- CSCsj01357

  Symptoms: Two network clock sources may serve the same backplane on a Cisco 7600 series, causing a loop that results in an incorrect clock time.

  Conditions: This symptom is observed when network clocking is configured and distributed to the line cards (that support network clocking) through the backplane and when the active and standby supervisor engines synchronize to the same back plane reference. The symptom occurs after multiple switchovers when the clock sources are configured and unconfigured.

  Workaround: No workaround.

- CSCsj01891

  Symptoms: When a diagnostic test (that is, a “scratch register test”) fails, a memory error may occur, and the Management Processor (NMP) may crash.

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

  Workaround: Disable the diagnostic test by entering the **diagnostic monitor** *module num* **test** *test-id* command.

  Further Problem Description: A scratch register test failure is a very rare failure that most likely indicates a hardware issue with one of the devices on the line card.

- 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

- CSCsj03474

  Symptoms: After you have changed a CEM group on a T1/E1 port of a SPA-24CHT1-CE-ATM from unframed to framed, traffic stops flowing through the port.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1.

  Workaround: Reload the SPA.

- CSCsj07328

  Symptoms: When IP interworking is configured on the first port of a PFC that is installed in slot 1 of the chassis of a PE router, an ARP request from a CE router may be not resolved.

  Conditions: This symptom is observed on a Cisco 7600 series that functions as a PE router.

  Workaround: Obtain the proxy MAC address on the PE router by entering the **show platform software xconnect mac-addr** command. On the CE router, use this MAC address as the destination IP address by using a static MAC address configuration.

  Alternate workaround: Move the interface to another port of the PFC in slot 1 of the chassis, or move the PFC to another slot.

- CSCsj07616

  Symptoms: A Route Switch Processor 720 (RSP 720) may generate the following error message and incorrect traceback while a CPU hog condition is being debugged:

  ```
  %CPU_MONITOR-SP-2-NOT_RUNNING_TB: CPU_MONITOR
  traceback:
  ```

  Conditions: This symptom is observed on a Cisco 7600 series when a failure occurs because of a CPU hog that is caused by a process or interrupt.

  Workaround: There is no workaround.

- CSCsj08843

  Symptoms: Line card information may be missing on the RP, and the following error message may be generated:

  ```
  %XDR-DFC9-6-XDRLCDISABLEREQUEST: Client XDR Interrupt Priority Client requested to be
  disabled. Due to XDR Keepalive Timeout
  ```

  Conditions: This symptom is observed on a Cisco router after you have repeatedly performed an OIR of the line card.

  Workaround: There is no workaround.

- CSCsj09790

  Symptoms: A line card crash and the following error messages may be generated:

  ```
  %INTR_MGR-DFC4-3-INTR: Queueing Engine (Blackwater) [0]: IPM Invalid packet ID
  %ESM20-DFC4-3-UNEXPECTED_GLOBAL_INT: Unexpected Global Interrupt:
  Blackwater_0/Icewater_0 Error %DFCWLC-DFC4-2-UNRECOVERABLE_FAILURE: DFC WAN Line Card
  Unrecoverable Failure for Device: Queueing Engine (Blackwater)
  ```

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

  Workaround: Remove the SPAN configuration.

- CSCsj10744

  Symptoms: The input queue for an interface on a SPA-2X1GE that is installed in a SIP-400 module may become wedged. When this situation occurs, the output of a **show** command shows the following information:

  ```
  GigabitEthernet2/2/1 is up, line protocol is up Input queue: 1076/75/61420/0
  (size/max/drops/flushes); Total output drops: 0
  ```

  The packets cannot be removed from the input queue. The packets remain in the input queue even after you have shut down and brought the interface.

  Conditions: This symptom is observed on a Catalyst 6000 series switch and Cisco 7600 series router that are configured for Web Cache Communications Protocol (WCCP), functioning in conjunction with the hardware NetFlow table.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs only on SPA interfaces, and only when NetFlow entries fail to install. Typically, this situation occurs when the NetFlow table is full. Each failed installation creates one entry in the input queue.

- CSCsj12034

  Symptoms: When you enter the **fabric switching-mode allow dcef-only** command on the active supervisor engine and you confirm that the standby supervisor engine must reload to change to dCEF mode, the standby supervisor engine does reload, comes up, but then enters ROMmon mode, and cannot be booted from ROMmon mode either.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that functions in SSO redundancy mode.

  Workaround: There is no workaround.

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

- CSCsj13343

  Symptoms: A router may crash when a SSO switchover occurs while you perform an OIR.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in an Xconnect configuration with 16,000 EVCs.

  Workaround: There is no workaround.

- CSCsj15638

  Symptoms: The standby supervisor engine may crash during bootup in SSO mode.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR when a large number of CEM circuits are configured with a CEM class is attached to them.

  Workaround: There is no workaround.

- CSCsj19194

  Symptoms: A Cisco 7600 series may crash when there are many link up/down flaps on a physical interface that has many VLANs associated.

  Conditions: This symptom is observed with the following large numbers of VLANs:

  - Number of existing VLANs: 4023
  - Number of existing VTP VLANs: 1005
  - Number of existing extended VLANs: 3018

  Workaround: There is no workaround.

Further Problem Description: Dequeueing of link up/down events that is handled by the “mls-gc” process occurs at a slower rate than the enqueueing. When the link flaps continue, memory that is allocated for each event is not freed in time, eventually causing the router to run out of memory and crash.

- CSCsj22790

  Symptoms: The power supply remains off when you perform an ISSU upgrade.

  Conditions: This symptom is observed on a Cisco 7600 series only when redundancy mode RPR is configured.

  Workaround: When redundancy mode RPR is configured, do not use ISSU. Rather, use FSU.

- CSCsj27140

  Symptoms: After you have performed an OIR, traffic may not flow on some interfaces of a SPA that is installed in a SIP-400.

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

  Possible Workaround: Reload the SPA or the SIP-400.

- CSCsj27414

  Symptoms: In a Service Control Engine (SCE) over MPLS configuration, when an input policy is configured to set the MPLS imposition experimental (EXP) bit and when the remote peer calls for AToM VC Type 4, the MPLS EXP bit imposition value is not copied into the Type 4 tag priority bits.

  Conditions: This symptom is observed on a Cisco 7600 series that has an Ethernet Services (ES20) line card when the remote peer (100.1.1.5 in the example below) is a Type 4 device. The ES20 line card does not copy the MPLS EXP bit imposition value into the inserted Type 4 dot1q tag. The symptom occurs in the following example configuration:

```
### sample configuration ###
class-map match-all MATCHANY
  match any
!
policy-map SETEXP
  class MATCHANY
   set mpls experimental imposition 5
!


!
interface GigabitEthernet2/0/0
 no ip address
 mls qos trust dscp
 service instance 1 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  service-policy input SETEXP
  xconnect 100.1.1.5 100 encapsulation mpls
 !
```

  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.

- CSCsj28277

  Symptoms: A platform ignores an IGMPv3 report when the first group address in the packet is 224.0.0.X. This situation causes other groups in the same packet to be ignored too, and, in turn, prevents a multicast stream from being forwarded.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch that has a Supervisor Engine 720 that runs Cisco IOS Release 12.(18)SXF8 but may also affect a Cisco 7600 series that runs Release 12.2SR.

  Workaround: Ensure that the end station that sends the IGMPv3 report lists any 224.0.0.x groups as the last group addresses in the report. If this is not an option, there is no workaround.

  Further Problem Description: The following is a sequence of a group record that fails:

```
Internet Group Management Protocol
    IGMP Version: 3
    Type: Membership Report (0x22)
    Header checksum: 0x09b0 [correct]
    Num Group Records: 2
    Group Record : 224.0.0.9  Mode Is Exclude
        Record Type: Mode Is Exclude (2)
        Aux Data Len: 0
        Num Src: 0
        Multicast Address: 224.0.0.9 (224.0.0.9)
    Group Record : 239.255.0.68  Mode Is Exclude
        Record Type: Mode Is Exclude (2)
        Aux Data Len: 0
        Num Src: 0
        Multicast Address: XXX.255.0.68 (xxx.255.0.68)
```

- CSCsj29413

  Symptoms: A router may not boot successfully because configurations for the ifIndex persistence are not read correctly from NVRAM.

  Conditions: This symptom is observed on a cisco 7600 series that has an RSP 720 that runs Cisco IOS Release 12.2SR and occurs only when the SNMP persistence database configuration is enabled.

  Workaround: The main reason for boot failure is the SNMP ifindex file corruption. This file is stored in NVRAM. The following sequence of commands clear the file from NVRAM and enables the RSP 720 to boot:

```
rommon 2> priv
rommon 3 > fill
Enter in hex the start address [0xfec00e00]:
Enter in hex the test size or length in bytes [0x100]:  0xeff200 Enter in hex the
pattern to be written [0x0]:  0xaaaaaaaa Enter the operation size "l"ong, "w"ord, or
"b"yte  [b]:  l
```

```
*** Data TLB Error Exception ***
PC = 0xfff98554, Vector = 0x1400, SP = 0x4013d24
Rommon 5>  b disk0:
```

- CSCsj29960

  Symptoms: After an SSO switchover has occurred, it may be impossible to connect to a CEoP SPA.

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

  Workaround: Reset the CEoP SPA.

- CSCsj30829

  Symptoms: When a Cisco 7600 series with a SIP-400 in which a POS SPA is installed is configured for Frame Relay encapsulation, traffic that is processed through Low Latency Queueing (LLQ) may be dropped because of a corrupt DLCI number.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB. The following is an example of a policy-map configuration in which the symptom occurs:

```
class-map match-any IP_VOICE_OUT
  match ip dscp ef


policy-map POLICY_V5
  class IP_VOICE_OUT
   police cir percent 5
    priority
  class class-default
```

  Workaround: Configure class-based weighted fair queueing (CBWFQ) with a police statement, as in the following example:

```
policy-map POLICY_V5
  class IP_VOICE_OUT
   police cir percent 5
    bandwidth percent 5
```

  Alternate Workaround: Do not use Frame Relay encapsulation. Rather, use HDLC or PPP encapsulation.

- CSCsj31272

  Symptoms: The following debug messages are generated on the console when you configure Xconnect on a module, even when debugs are not enabled:

```
Skipping setup switching for Ethernet interface <name>
  List Enqueue Failed Add to Hotstandby Q
  List Remove Failed Remove from HeldQ
  deallocate segment <num>
  unprovision switch <num>
```

  Conditions: This symptom is observed on a Cisco router after an RP switchover has occurred.

  Workaround: There is no workaround.

- CSCsj33346

  Symptoms: A Cisco 7600 series switching processor (SP) may fail to generate a crashinfo file.

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when **exception crashinfo** global configuration commands are executed and when the configuration is saved.

Workaround: Do not add a configuration with **exception crashinfo** global configuration commands.

- 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.

- 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.

- 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.

- CSCsj38436

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

  ```
  %ICC-2-NOMEM: No memory available for asynchronous request
  -Traceback= 4062ACB8 4062B1FC 423318EC 42331F6C 42332160 421DDCF4 421EB12C 422BE264
  422BE634 412DAB40 412FC674 412DB7B8 412DC12C 412B7EB4 412B8038 412B7CAC
  ```

  After the error message and traceback have been generated, the CPU usage increases, and eventually the router crashes.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1 when you de-activate and re-activate SLB-GTP and SLB-FWLB and run traffic for GSM users through SLB-GTP and SLB-FWLB for several hours.

  Workaround: There is no workaround.

- CSCsj38796

  Symptoms: When you boot the platform, the supervisor engine and a line card may crash during the “label_entry_get_inlabel” process.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured for MPLS.

  Workaround: There is no workaround.

- 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.

- CSCsj46613

  Symptoms: When the standby supervisor engine is reset, a memory leak may occur on the active supervisor engine.

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

  Workaround: There is no workaround.

- CSCsj46965

  Symptoms: Diagnostic scheduling may not be effective after forced switchover.

  Conditions: This symptom is observed on a Cisco 7600 series that has a 1-port OC-12c/STM-4c ATM SPA (SPA-1XOC12-ATM).

  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.

- CSCsj47551

  Symptoms: When you enter the **interface range** command, the standby supervisor engine may reset unexpectedly.

  Conditions: This symptom is observed on a Cisco router that is configured for high availability (HA).

  Workaround: There is no workaround.

- CSCsj55688

  Symptoms: A WAN line card may fail to boot when the following error condition occurs:

  ```
  %ETSEC-5-LATECOLL: PQ3/FE(0), Late collision
  ```

  The late collision error is result of a delay in the collision signal that is received by the MAC address of the line card.

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

  Workaround: There is no workaround.

- 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.

- CSCsj58287

  Symptoms: A SPA services carrier card (7600-SSC-400) may crash after a reload.

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

  Workaround: There is no workaround.

- CSCsj58538

  Symptoms: Line protocol flaps may occur on a router after an SSO switchover. This situation causes traffic loss for a short time until the interfaces come back up and traffic is restored.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in a highly scaled environment and that has many interfaces are configured.

  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.
  ```

- CSCsj60582

  Symptoms: 802.1q tags may be misordered when Xconnect is configured on an service instance that is configured on an Ethernet Services (ES20) line card. When this situation occurs, the misordered 802.1q tags are sent to the MPLS core and the remote EoMPLS peer.

Conditions: This symptom is observed on a Cisco 7600 series when all of the following conditions are present:

- The **rewrite ingress tag** command with a "push dot1q" tag manipulation is configured on the interface. Both single and double tags are affected.
- The **xconnect** *ip-address* **encap mpls** is configured on the service instance.
- The remote peer has negotiated VC Type 4 (Ethernet+VLAN) rather than VC Type 5 (Ethernet only).

Workaround: There is no workaround.

Further Problem Description: The following is an example of an interface configuration with a "push dot1q" tag manipulation:

```
interface GigabitEthernet2/0/0
 no ip address
 no mls qos trust
 no cdp enable
 spanning-tree bpdufilter enable
 service instance 100 ethernet
  encapsulation dot1q 100
  rewrite ingress tag push dot1q 105 symmetric
  xconnect 10.1.1.5 100 encapsulation mpls
 !
```

The following is an example of a VC Type 4 (Ethernet+VLAN) peer configuration:

```
router#sh mpls l2 binding
  Destination Address: 10.1.1.5,  VC ID: 100
    Local Label:  21
        Cbit: 0,    VC Type: Eth VLAN,    GroupID: n/a
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: RA [2]
              CV Type: LSPV [2]
    Remote Label: 18
        Cbit: 0,    VC Type: Eth VLAN,    GroupID: 0
        MTU: 1500,   Interface Desc: n/a
        VCCV: CC Type: None
              CV Type: None
```

- CSCsj64490

  Symptoms: After you have reloaded the router, some ports on an Ethernet Services (ES20) line card may remain in the down/down state.

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

  Workaround: Reload the line card.

- CSCsj65755

  Symptoms: Packet loss may occur, and an "SPI NOT Available" error message may be generated during a rekey.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with an IPSec VPN SPA and occurs under either one of the following conditions:

  - when the first rekey after a switchover or revert back occurs.
  - when any SA setup occurs during a switchover or revert back.

Workaround: There is no workaround.

- CSCsj67110

  Symptoms: A router may crash or report an error message similar to the following:

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

  This can be seen for a process other than the “draco-oir” process.

  Conditions: This symptom is observed on a Cisco 7600 series when HSRP is configured. The symptom occurs when there is an event that requires the HSRP configuration to be removed, for example, when you perform an OIR of a module while the **module clear-config** command is enabled. The interface with HSRP does not have to be up for the symptom to occur.

  Workaround: Remove the HSRP configuration before you perform an OIR.

  Alternate workaround: Enter the **no module clear-config** command. (The **module clear-config** command is enabled by default. You must enter **no** form of the command to disable it.)

- CSCsj67336

  Symptoms: A Cisco 7600 series may crash when you perform an OIR of a line card such as a SIP-400 or Ethernet Services (ES20) line card that contains an SFP transceiver.

  Conditions: This symptom is observed when the SFP transceiver has DOM capability.

  Workaround: First, remove the SFP transceiver. Then, perform an OIR of the line card.

- CSCsj68502

  Symptoms: A SPA-24CHT1-CE-ATM for which no card type is configured may crash when you configure an out-of-band clock (that is, when you configure a clock master and slave).

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.(33)SRB1.

  Workaround: First, configure the card type for the SPA-24CHT1-CE-ATM. Then, configure an out-of-band clock.

- 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.

- CSCsj70658

  Symptoms: Counters on 4th interface of a WS-X6704-10GE module may report incorrect traffic levels after 3.4 Gbps of traffic has been exceeded in any one direction.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1.

  Workaround: Apply a policy map on the interface to provide correct reporting of the traffic levels.

- CSCsj72723

  Symptoms: The link LED of an Ethernet Services (ES20) line card or an Ethernet SPA that is installed in a SIP-600 may continue to light green even when the port is shut down.

  Conditions: This symptom is observed on a Cisco 7600 series after you have reloaded the line card, the SPA, the SIP-600, or the router.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not impact the functionality of the router because no traffic passes through the port that is shut down even though the LED continues to light green.

- CSCsj73785

  Symptoms: A VLAN check flag is not set for MPLS adjacencies or when incoming packets are routed on the same interface. When this VLAN check failure occurs, packets are punted to RP.

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

  Workaround: There is no workaround.

  Further Problem Description: In an IP-to-IP configuration, you can prevent the symptom from occurring by entering the **no ip redirect** command on the interface. However, when packets are sent from IP to MPLS, this command does not take effect.

- CSCsj78751

  Symptoms: When you enter the **shutdown** command followed by the **no shutdown** command on a 10-Gigabit XFP transceiver module that is installed in an Ethernet Services (ES20) line card, the transceiver module may remain in the down/down state.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1 and that has a ES20 line card with a 2x10GE XFP an a DFC 3CXL (7600-ES20-10G3CXL). The symptom occurs only with a 10-Gigabit XFP transceiver module from a particular third-party vendor.

  Workaround: Reset the line card by entering the **hw-module module** *slot-number* **reset** command.

- CSCsj82497

  Symptoms: ATM subinterface statistics are not preserved when the VC is recreated, and are reset to zero.

  Conditions: This symptom is observed on a Cisco router when the VC is recreated, for example, because of a bandwidth or encapsulation change on the VC.

  Workaround: There is no workaround.

- CSCsj84781

  Symptoms: When multicast is configured on a Cisco router, the following error message may be generated in the log:

  ```
  %IPRT-3-NDB_STATE_ERROR: NDB state error (BAD EVENT STATE) (0x8001) 20.0.5.0/24,
  state 7, event 0->1, nh_type 1 flags 4
  - Process= "Exec", ipl= 0, pid= 3
  ```

  Conditions: This symptom is observed when multicast is enabled, that is, when at least one interface is configured with a multicast protocol, and when a route exists as both a unicast route and a native multicast route. For example, the symptom may occur when the following sequence of events occurs:

  - 10.0.0.0 255.0.0.0 is learned in unicast via an IGP.
  - You then configure the same router as a multicast static route:

    ```
    ip route 10.0.0.0 255.0.0.0 192.168.200.1 multicast
    ```

  - Reachability to the multicast route flaps.

  Workaround: There is no workaround.

  Further Problem Description: In addition to the conditions that are stated above, the set of prefixes in the multicast routing table has certain distribution properties. A variety of cases can meet the criteria which are not easily described.

- CSCsj85463

  Symptoms: When a large number of subinterfaces are configured on an interface of an Ethernet Services (ES20) line card and when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface, high CPU usage may occur on the switch processor and/or line card.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB or Release 12.2(33)SRB1.

  Workaround: There is no workaround.

- 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”.

- CSCsj89208

  Symptoms: A TLB exception may occur on the RP when you perform an OIR of a SIP-400.

  Conditions: This symptom is observed on a Cisco 7600 series when a SPA-2X1GE-V2 SPA with a total of 8000 Ethernet virtual connections (EVCs) (4000 per port) is installed in the SIP-400.

  Workaround: There is no workaround.

- CSCsj90451

  Symptoms: When the **mpls ip** interface configuration command is enabled on an interface, the processing of traffic to an MPLS cloud may cause high CPU usage at the interrupt level.

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1. The symptom occurs because of an incorrect hardware adjacency for a route that was learned via BGP.

Workaround: Disable the **mpls ip** interface configuration command.

- CSCsj91795

  Symptoms: An application traffic class may not be monitored passively but can only be monitored actively. In addition, application traffic cannot be used for load-balancing.

  Conditions: These symptoms are observed in an optimized edge routing (OER) configuration with a Cisco router that functions as a master controller (MC) that runs Cisco IOS Release 12.4(15)T and a border router (BR) that runs Release 12.2(33)SRB.

  Workaround: Use the active monitoring mode for the performance policy. There is no workaround to load-balance application traffic.

- 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.

- CSCsj92153

  Symptoms: Prolonged high CPU usage may occur in the “Tag Control” process in steady-state conditions and in the “IP RIB Update” process during route change events.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that function in a network environment with large numbers of BGP routes such as more than 100,000 BGP routes.

  Workaround: There is no workaround. However, if BGP next-hop tracking is enabled, disable it. Doing so helps to alleviate the high CPU usage because there are less route change events.

- CSCsj93195

  Symptoms: A bus error may occur on an MSFC when ISAKMP is enabled, and the following error message may be generated in the logs:

  ```
  %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON Address Error (load or instruction fetch)
  exception, CPU signal 10, PC = 0x41579EB0
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that has a Supervisor Engine 720 and that runs Cisco IOS Release 12.2(33)SRA2.

  Workaround: There is no workaround.

  Further Problem Description: Cisco IOS Release 12.2(33)SRAs 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)SRA2 on a Cisco Catalyst 6500 series switch, the symptom may occur.

- CSCsj93495

  Symptoms: A memory leak may occur on a router that functions in an AToM configuration with Virtual Forwarding Instances (VFIs).

Conditions: This symptom is observed on a Cisco router in a scaled configuration when link flaps occur.

Workaround: There is no workaround.

- CSCsj95033

  Symptoms: When a virtual routing and forwarding (VRF) instance is deleted from a configuration, the memory of the VRF is not freed. This situation causes a leak in the processor memory.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that is based on Release 12.2S when a VRF instance is created and then deleted or when CEF is enabled and then disabled.

  Workaround: Configure the router in such a way that VRF instances are not deleted and that CEF is not enabled and disabled.

- CSCsj95268

  Symptoms: A CPUHOG warning is logged for the environment polling process.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1 and could occur because the CPU is busy when the environment polling process runs.

  Workaround: There is no workaround. Note that the router recovers by itself.

- CSCsk01407

  Symptoms: A CEoP SPA may not come up.

  Conditions: This symptom is observed on a Cisco 7600 series that has a CEoP SPA with a golden FPGA image that is corrupted, which may be related to the frequency of FPD updates.

  Because the corrupt golden FPGA image is only required if a failure occurs during the FPD update process, the corruption may be present for a long period of time before being detected.

  Workaround: There is no workaround. When a golden image is corrupted and when an FPD update failure occurs, the SPA does not boot.

  Further Problem Description: Note that the most frequent cause of FPD failures is a mismatch between the FPD image bundle and the running Cisco IOS software image. (FPD image bundles that support Release 12.2(33)SRB are incompatible with subsequent software images.)

- CSCsk01927

  Symptoms: A VC on a PE router remains up after you have shut down the ATM interface on a connected CE router.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that has the **oam-ac emulation-enable** command enabled.

  Workaround: There is no workaround.

- CSCsk02933

  Symptoms: When a multiple path RPF interface group is configured, all interfaces in this group should use distributed cache for a known source address. However, in this situation, packets may processed in route cache on one of the interfaces, which is improper behavior.

  Conditions: This symptom is observed on a Cisco 7600 series that has three or more interfaces configured in a multiple path RPF interface group and occurs after you have entered the **issu runversion** command as part of an ISSU, causing the new standby supervisor engine to become active. Note that the symptom does not yet occur when you enter the **issu loadversion** command but only after you have entered the **issu runversion** command.

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 the affected interface.

- CSCsk04241

  Symptoms: When you enable the laser on a 10GE interface of an Ethernet Services (ES20) line card that is installed in a SIP-600, the XFP may enter a "not ready" state, causing the 10GE interface to remain in the down/down state.

  Conditions: This symptom is observed on a Cisco 7600 series after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the 10GE interface.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, perform a physical OIR of the line card.

- CSCsk08750

  Symptoms: During an SNMP walk that queries the IF-MIB::ifLastChange instance, the timeticks show a value of zero. When you verify this result against the MIB::sysUpTimeInstance, it does not match. Other interfaces have a valid "ifLastChange" instance value.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB1 when an SNMP walk is performed on the ifLastChanged MIB for a 4-port channelized T3 to DS0 SPA (SPA-4XCT3/DS0).

  Workaround: There is no workaround.

- 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.

- CSCsk16706

  Symptoms: Interface configuration changes on the active supervisor engine may be rejected with the following error message:

  ```
  %ERROR: Standby doesn't support this command
  ```

  Conditions: This symptom is observed on a Cisco 7600 series when a line card is reset while the standby engine is still booting up to its terminal state in SSO or RPR-plus (RPR+) operating mode.

  Workaround: Reboot the standby supervisor engine.

- CSCsk21925

  Symptoms: Both the primary and backup tunnels pass traffic when the primary tunnel is still active and when you have entered the **no shutdown** command on the backup tunnel. This situation causes traffic to reach the peers via both the primary and backup tunnels.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for FRR.

  Workaround: There is no workaround.

- CSCsk22554

  Symptoms: You may not be able to unconfigure a switchport on an Ethernet Services (ES20) line card.

  Conditions: This symptom is observed on a Cisco 7600 series after you first have configured and unconfigured an EFP on an ES20 line card, and then you configure and attempt to unconfigure a switchport.

  Workaround: There is no workaround.

- CSCsk37096

  Symptoms: When there are many Xconnect attachment circuits or VFIs configured on a router, the following error message may be generated on startup:

  ```
  Task is running for (2000)msecs, more than (2000)msecs (4465/4464),process = CDP
  Protocol.
  ```

  Conditions: This symptom is observed on a Cisco router only when there are several thousand Xconnect attachment circuits or VFIs configured.

  Workaround: There is no workaround. However, the message is harmless and can be ignored.

- CSCsk37110

  Symptoms: When there are 1000 to 4000 VFIs configured and when an SSO switchover occurs, multiple tracebacks may be generated on the new primary RP, and there is long delay before the VCs start to switch packets.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB in a configuration with two RPs that function in SSO mode.

  Workaround: There is no workaround.

- CSCsk39340

  Symptoms: High CPU usage may occur when the IP Rewrite Manager (IPRM) is active.

  Conditions: This symptom is observed on a Cisco router when there is a large number of prefixes and when there is network instability.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat alleviates the high CPU usage.

- CSCsk43336

  Symptoms: BGP routes that are reachable via a next hop over a traffic engineering (TE) tunnel may be removed from the RIB for up to one hour when the physical interface on which the TE tunnel is configured flaps.

  Conditions: This symptom is observed on a Cisco router when a link state IGP (IS-IS or OSPF) is configured to use TE tunnels and when the physical interface on which the IGP has a neighbor and that is part of the Label Switched Path (LSP) for the TE tunnel flaps. The symptom occurs when the IGP neighbor is restored and when the TE tunnel comes up before IGP reinstalls the routes that were affected by the interface flap. In this situation, BGP may not be informed about the reachability of the BGP next hop.

  Workaround: There is no workaround. The BGP routes will eventually be restored as a result of a background check that is performed by BGP, but this may take up to an hour.

  Further Problem Description: The symptom does not occur when no multicast protocol is configured.

- CSCsk44055

  Symptoms: After a router has been reloaded, traffic may no longer pass on an interface that has the **switchport trunk encapsulation dot1q** command enabled.

  Conditions: This symptom is observed on rare occasions on a Cisco 7600 series that has a Route Switch Processor 720 (RSP720).

  Workaround: Reset the line card. If this is not an option, there is no workaround. Reloading the router is not a workaround.

  Further Problem Description: The symptom does not on a Cisco 7600 series that has a supervisor engine.

- CSCsk45057

  Symptoms: Layer 2 traffic flooding stops after you have removed a VLAN from the database and then added the VLAN to the VLAN database on a SIP-400. The following is an example of a sequence of commands that causes the symptom to occur:

  ```
  config t
  no vlan vlanid
  vlan vlanid
  exit
  ```

  Conditions: This symptom is observed on a Cisco 7600 series when the core-facing interface is in the label imposition path of an VPLS or EoMPLS VC. Note that traffic that is destined for a known MAC address is not affected.

  Workaround: Enter the following sequence of command to restore the traffic:

  ```
  config t
  interface vlan vlanid
  shutdown
  no shutdown
  ```

- CSCsk48565

  This caveat consists of two symptoms, one condition, and one workaround:

  Symptom 1: When both Distributed Compressed Real-Time Protocol (dCRTP) and QoS are configured, compression does not occur, and the output of the **show ip rtp header-compression** command shows all counters as zero.

Symptom 2: When the **ppp multilink fragment-delay 8** command is configured on an MLP interface, packets are wrongly fragmented.

Conditions: These symptoms are observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

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.

- CSCsk53232

  Symptoms: When you reconfigure a POS interface on a SIP-400 from BCP (PPP) bridging to Frame Relay bridging, traffic may not flow.

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

  Workaround: Reload the SIP-400 microcode or reload the SIP-400.

- CSCsk54783

  Symptoms: A Cisco 7600 series may crash when many transmission errors occur in the network and when the router processes a corrupt packet with a size of 9 bytes carries a partial RFC1483 header.

  Conditions: This symptom is observed on a Cisco 7600 series with a SIP-400 in which a ATM SPA is installed that is configured for MPB. YOu can check the SPA error counters to determine the transmission errors.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs when, after the router has received the corrupt packet, the network processor sends a short-length packet to the Encoded Address Recognition Logic (EARL) engine, which, in turn, triggers the Hyperion ASIC to reset.

- CSCsk56395

  Symptoms: A VC on a PE router remains up after you have shut down the ATM interface on a connected CE router, and the **oam-ac emulation-enable** command does not show in the output of the **show running-config** command.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that has the **oam-ac emulation-enable** command enabled.

  Workaround: There is no workaround.

- CSCsk57114

  Symptoms: CPUHOG messages may be generated when an “snmpwalk” is performed on the cpwVcMplsNonTeMappingTable object.

  Conditions: This symptom is observed on a Cisco router that has a large number (about 30,000) of pseudowires configured.

  Workaround: Reduce the number of pseudowires that are configured on the router.

- CSCsk59014

  Symptoms: When a bridge domain service instance is configured at boot time, the Switch Virtual Interface (SVI) remains in the down state.

Conditions: This symptom is observed on a Cisco 7600 series that has a SIP-400 that is configured for Multipoint Bridging (MPB).

Workaround: There is no workaround.

- CSCsk62662

  Symptoms: After the router is reloaded, traffic may not be forwarded by one of the line cards. An end-to-end ping may also fail.

  Conditions: This symptom is observed on rare occasions on a Cisco 7600 series that has a Route Switch Processor 720. The symptom does not occur with other supervisor engines.

  Workaround: Reset the line card.

- 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.

- CSCsk72529

  Symptoms: After you have initiated an SSO switchover by entering the **redundancy force-switchover** command, layer 2 traffic flooding stops on the redundant supervisor engine after you have removed a VLAN from the database and then added the VLAN to the VLAN database on a SIP-400. The following is an example of a sequence of commands that causes the symptom to occur:

  ```
  config t
  no vlan vlanid
  vlan vlanid
  exit
  ```

  Conditions: This symptom is observed on a Cisco 7600 series when the core-facing interface is in the label imposition path of an VPLS or EoMPLS VC Note that traffic that is destined for a known MAC address is not affected.

  Workaround: Enter the following sequence of command on the redundant supervisor engine to restore the traffic:

  ```
  config t
  interface vlan vlanid
  shutdown
  no shutdown
  ```

- CSCsk74750

  Symptoms: The standby supervisor engine may crash when you perform an OIR of an Ethernet Services (ES20) line card that has a highly scaled configuration.

  Conditions: This symptom is observed on a Cisco 7600 series that has an ES20 line card (as part of a 7600-ES20-D3CXL bundle) that is configured with 2000 Software Ethernet over MPLS VCs, 4000 Scalable Ethernet over MPLS VCs, and 500 Hardware Ethernet over MPLS VCs.

  Workaround: There is no workaround.

- 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.

TCP/IP Host-Mode Services

- 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.

- CSCsi70599

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

  1. Symptom 1: When you create a dynamic Frame-Relay map and remove it by entering the **no frame-relay map** command, the standby RP may reboot unexpectedly.

     Condition 1: This symptom is observed on a Cisco 7600 series. However, the symptom may be platform-independent.

     Workaround 1: Do not enter the **no frame-relay map** command to remove a dynamic Frame-Relay map. Rather, enter the **clear frame-relay inarp** command.

2. Symptom 2: When you create a dynamic Frame-Relay map and remove it by entering the **no frame-relay map** command, the router may generate the following error message:

   ```
   %REDUNDANCY-3-CONFIG_SYNC: Active and Standby lbl configuration out of sync
   ```

   Condition 2: This symptom is observed on a Cisco 12000 series. However, the symptom may be platform-independent.

   Workaround 2: Do not enter the **no frame-relay map** command to remove a dynamic Frame-Relay map. Rather, enter the **clear frame-relay inarp** command.

- 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)SRB1

Cisco IOS Release 12.2(33)SRB1 is a rebuild release for Cisco IOS Release 12.2(33)SRB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRB1 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCin93236

  Symptoms: The CPU usage of the TACACS+ process may be high.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCeh31423. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh31423. 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.

- CSCir01788

  Symptoms: The **ip-tacacs source-interface** command is missing from the command line interface (CLI).

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

  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.

- CSCsd49317

  Symptoms: When you enter the **no tacacs-server administration** command, the router may crash because of processor memory corruption.

  Conditions: This symptom is observed when you enter the **no tacacs-server administration** command while the **tacacs-server administration** command was not previously configured.

  Workaround: Do not enter the **no tacacs-server administration** command while the **tacacs-server administration** command was not previously configured.

- CSCsh72214

  Symptoms: A router may reject a valid username and password during the authentication of a console or vty session.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when the **aaa authentication login local** is configured on the console or vty.

  Workaround: Configure authentication by entering the **aaa authentication login default local** command, which still enables the local username database on the router for authentication.

Interfaces and Bridging

- CSCed79345

  Symptoms: A router crashes when you enter the **default/no bridge-group** *bridge group* **subscriber-loop-control** interface configuration command.

  Conditions: This symptom is observed when there are no existing bridge-group configurations on the router.

  Workaround: There is no workaround.

- 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.

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.

- 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. However, the symptom is not platform-dependent.

  Workaround: There is no workaround.

- CSCek68270

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

  Conditions: This symptom is observed on a Cisco router that contains an 0.0.0.0/0 address in the EIGRP topology with multiple next hops that change in quick succession.

  Workaround: Limit the 0.0.0.0/0 address to a single next hop.

- CSCek68507

  Symptoms: A router that has the **ip multicast limit** command enabled may crash when you enter the **show running-configuration** command.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB but is both platform- and release-independent. When you remove or re-enable a tunnel or virtual interface that has the **ip multicast limit** command enabled, a spurious memory access may occur, and the router may crash.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCse51804

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

Symptom 1: A DMVPN tunnel may flap at regular intervals. The NHRP cache entry at the hub expires a long time before its expiration time.

Condition 1: These symptoms are observed on a Cisco router that runs Cisco IOS Release 12.4 when the DMVPN tunnel is up and when you enter the **show ip nhrp brief** and **clear ip nhrp** commands. When the tunnel comes up again (because of the NHRP registration by the spoke), the NHRP cache entry expires a long time before its expiration time.

Workaround 1: Do not enter the **show ip nhrp brief** command.

Symptom 2: A DMVPN tunnel may flap at regular intervals. The NHRP cache entry at the hub expires a long time before its expiration time.

Condition 2: These symptoms are observed on a Cisco router that runs Cisco IOS Release 12.4(6)T or a later release and occurs without any specific action.

Workaround 2: There is no workaround.

Further Problem Description: These symptoms are not release-specific.

- CSCsg83966

  Symptoms: Paths that are imported via VPN may be missing from the VRF. For example, paths that are imported from the same route distinguisher (RD) may be missing from the VRF.

  The route map that is specified in the **import ipv4 unicast map** *route-map* command is meant to be applied to paths that are imported into the VRF from the global table. However, the route map is also incorrectly applied to VPN paths during the VPN import process. When the route map filters some of these paths, they are not imported, which is shown in the output of the **show ip bgp vpnv4 vrf vpn-name** command.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when you use the **import ipv4 unicast map** *route-map* command to import an address family from the global table into a VRF. The following sequence of events illustrates how the symptom occurs:

  1. Configure an IP prefix list. [example: ip prefix-list COLORADO seq 5 permit 10.1.5.0/24]
  2. Configure a route map by using the prefix list as the matching criteria. [example: route-map UNICAST permit 10 match ip address prefix-list COLORADO]
  3. Import the route map into the VRF. [example: ip vrf isp1 rd 65031:100 import IPv4 Unicast map UNICAST route-target export 65031:100 route-target import 65031:100]
  4. Trigger a routing update by entering the **clear ip bgp** command.
  5. Check the output of the **show ip bgp vpnv4 vrf vpn-name** command. The output does not show entries from the BGP neighbor.

  Workaround: There is no workaround.

- CSCsh02161

  Symptoms: A Route Reflector (RR) does not withdraw a prefix that redistributes itself even if this prefix is removed from the BGP table.

  Conditions: This symptom is observed on a Cisco router that functions as an RR that advertises two of the same prefixes with different Route Distinguishers (RDs) when one of these prefixes redistributes itself and when the other prefix is a route that is learned from an RR client via iBGP.

  Workaround: There is no workaround.

- CSCsh17035

  Symptoms: A route may flap continuously and the CPU usage may be high continuously.

Conditions: This symptom is observed on a Cisco router that is configured with a static route loop.

Workaround: Do not configure a static route loop.

- 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.

- CSCsh65136

  Symptoms: RSVP reservations may become lost or may not be rebuilt when an SSO switchover occurs. Although RSVP is not SSO-aware, RSVP reservations should be re-established after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with dual Supervisor Engine 720 modules and a Policy Feature Card 3BXL (PFC3BXL) and that functions in the following configuration:

  - The Cisco 7600 series functions as a mid-point router.
  - The router that sends RSVP reservations is a downstream router.
  - The router that should receive the RSVP reservations is an upstream router and is enabled for RSVP CAC.

  The interfaces that are used in the topology are Gigabit Ethernet interfaces and 10-Gigabit Ethernet with subinterfaces.

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

- CSCsh66294

  Symptoms: A Cisco 7600 series that is configured for BGP crashes during normal operation.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that functions as a PE router in an MPLS environment.

  Workaround: There is no workaround.

- CSCsh91798

  Symptoms: After you have unconfigured a VRFm, the VRF may not be removed properly and remain in the "delete pending" state.

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

  Workaround: There are no workaround.

ISO CLNS

- CSCek69976

  Symptoms: An IS-IS adjacency message may not be copied correctly between the active RP and the standby RP.

  Conditions: This symptom is observed on a Cisco router when an In Service Software Upgrade (ISSU) is performed between a Cisco IOS software image with IS-IS ISSU support for adjacency message version 2 and a Cisco IOS software image with IS-IS ISSU support for adjacency message version 4.

Workaround: There is no workaround.

- 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

- 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.

- CSCek28110

  Symptoms: XDR tracebacks are generated after an SSO switchover has occurred.

Conditions: This symptom is observed on a Cisco router and seems to occur only after multiple SSO switchovers have occurred.

Workaround: There is no workaround.

- CSCek63433

  Symptoms: An MSFC bus error crash may occur, and the following error message may be generated:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x40B96C4C
  ```

  Conditions: This symptom is observed when multiple processes share a socket, causing the RP to crash during the exit of these processes.

  Workaround: There is no workaround.

- CSCek64847

  Symptoms: On a router that is configured for Hot Standby Router Protocol (HSRP), the hold timer that is configured via the **standby timers msec** command does not function properly when the standby group number is 17 or higher.

  The configured standby hold time changes unexpectedly to 3 times the group number value instead of remaining in the 50-3000 msec range when the standby group is configured in the 17-4095 range.

  Also, when a relatively high number is configured for the standby group, a "%PARSER-4-BADRANGE" error message is generated.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(6)T3 or Release 12.4(11)T but may also affect other releases such as Release 12.2SR.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.4(5a).

- CSCek65022

  Symptoms: A 7600-SSC-400 SPA services carrier may crash during the boot process of a SPA.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when an IPsec VPN Shared Port Adapter (SPA-IPSEC-2G) that is installed in the 7600-SSC-400 boots.

  Workaround: There is no workaround.

- CSCek66114

  Symptoms: After an SSO switchover has occurred, the standby supervisor may not come up because the startup configuration does not synchronize to the standby supervisor.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB after a single or multiple SSO switchovers have occurred.

  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.

- CSCek66294

  Symptoms: The TCP MSS Adjustment feature works only in the ingress direction. The feature should work both in the ingress and egress direction.

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

  Workaround: There is no workaround.

- CSCek66731

  Symptoms: On a Cisco 7600 series packets that are received by a routed interface that does not have an IPv4 address may be forwarded by CEF.

  Conditions: This symptom is observed when the Cisco 7600 series receives an IP packet on an interface that has no IPv4 address enabled but that has a matching route entry to forward the packet to a destination.

  Workaround: Shut down the interface that has no IPv4 address enabled.

- CSCek67622

  Symptoms: The **bfd interval** command is accepted on EtherChannel and EtherChannel member interfaces.

  Conditions: This symptom is observed on a Cisco router while BFD is not supported on EtherChannels.

  Workaround: Do not enter the **bfd interval** command on EtherChannel and EtherChannel member interfaces.

- 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.

- CSCek68017

  Symptoms: When more than 4000 entries are allocated in a VPN table in an MPLS configuration, the following error message may be generated:

  ```
  %VPNMAP-SP-2-SPACE_EXCEEDED
  ```

  Conditions: This symptom is observed on a Cisco 7600 that runs Cisco IOS Release 12.2(33)SRB when EoMPLS VCs boot or when the router is configured with IPv4 VRFs. The symptom occurs irrespective of whether or not IPv6 is configured.

  Workaround: There is no workaround.

- CSCek68370

  Symptoms: An Xconnect interface that is configured on an Ethernet Virtual Circuit (EVC) may remain down.

  Conditions: This symptom is observed when the encapsulation is set to default or untagged.

  Workaround: There is no workaround.

- CSCek68853

  Symptoms: On a Cisco 7600 series that has redundant Supervisor Engine 32 modules, the standby supervisor engine reloads unexpectedly during the boot process and generates the following error message:

  ```
  %RF-SP-3-NOTIF_TMO: Notification timer Expired for RF Client: Cat6k CAPI(1317)
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that functions in SSO mode, that has a scaled Multipoint Bridging (MPB) configuration with 16,000 ATM MPBs and 4000 Frame Relay MPBs, and that is configured for Circuit Emulation over Pseudowires (CEoP), Virtual Private LAN Services (VPLS), and other features.

  Workaround: There is no workaround.

- CSCek68959

  Symptoms: When a second RPR+ switchover occurs and when an OSM-2+4GE-WAN+ module resets during the switchover, the running configuration may become lost on the OSM-2+4GE-WAN+ module. When this situation occurs, the interfaces and the L2 and L3 VPNS that are configured on the OSM-2+4GE-WAN+ module do not come up, and traffic that is processed over these interfaces and VPNS becomes lost.

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

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, copy the startup configuration to the running configuration.

- CSCek69134

  Symptoms: When you enter the **default interface** command on an interface with a scaled Ethernet Virtual Circuit (EVC) service instance configuration, it may take a long time for the command to be executed, and during this time, the CPU usage of the RP may increase to 100 percent. In addition, many error messages may be generated.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when a scaled EVC service instance configuration is enabled on a Gigabit Ethernet port of a 20-port Ethernet Services line card (7600-ES20-GE) that is installed in a SIP-400.

  Workaround: There is no workaround. You must wait until the command has been executed. However, the command functions properly.

  Further Problem Description: The **default interface** command is often used to set an interface to its default state before a configuration is applied, and it is used to remove a scaled configuration from an interface by just entering one command rather than deleting individual configuration lines one-by-one.

  As an alternative, you can enter the **no service instance** command for each service instance on the port. The following example shows steps to simplify the process:

  Instead of entering the **default gi1/0/1** command, do the following:

  1. Enter the **show running interface gi1/0/1 | inc service instance** command.
  2. Cut-and-paste the output into your preferred editor.
  3. Edit the file by placing “no” before each line.
  4. Enter the following configuration:

     conf t int gi1/0/1 <*paste the file*>

     or just copy the file to running configuration.

- CSCek69280

  Symptoms: When you initiate an SSO switchover after several ISSU transitions have been executed, a SIP-400 may reload unexpectedly. When this situation occurs, the following error message is generated:

  ```
  %OIR-SP-3-PWRCYCLE: Card in module 9, is being power-cycled off (Reset - Module
  Reloaded During Download)
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with redundant Route Switch Processor 720 (RSP720) cards after the following sequence of commands has been executed:

  issu loadversion issu abortversion redundancy force-switchover

  or the following sequence of commands:

  issu loadversion issu runversion issu acceptversion issu abortversion redundancy force-switchover

  Workaround: Do not use the **issu abortversion** command.

  Further Problem Description: The SIP-400 does not normally reload when the **redundancy force-switchover** command is executed. The SIP-400 reloads only if first a sequence of ISSU transitions is performed, and then the **redundancy force-switchover** command is executed.

- CSCek69641

  Symptoms: When you perform an ISSU downgrade after an ISSU upgrade has occurred, a 10-Gigabit Ethernet Switching Module (WS-X6704-10GE) may crash, and the following error messages may be generated:

  ```
  SP: PREDNLD_ERRMSG: IPC: Failed to tx image pkt to IPC port Slot 9/0: REDNLD: retry
  queue flush [for 9/0]
  ```

  ```
  %OIR-SP-6-NOPWRISSU: Card inserted in slot 9 powered down because ISSU is in progress
  ```

  ```
  %MDR_SM-SP-3-SLOT_NOTIFY_TIMEOUT: Notification timeout on MDR slot state machine 9
  for the local client Last SP MDR client (1) in state SLOT_PREDOWNLOAD
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with redundant Route Switch Processor 720 (RSP720) cards after the following sequence of commands has been executed:

  First, you perform and ISSU upgrade to the new Cisco IOS software image:

  ```
  issu loadversion
  issu abortversion
  issu runversion
  issu acceptversion
  issu commitversion
  ```

  Then, you perform and ISSU downgrade to the old Cisco IOS software image:

  issu loadversion

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **issu abortversion** command and restart the ISSU downgrade procedure by entering the **issu loadversion** command.

- 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.

- CSCek70210

  Symptoms: Control word information may not be programmed on the forwarding table, causing a datapath failure through an EoMPLS VC.

  Conditions: This symptom is observed very rarely on a Cisco 7600 series that has a VC that is configured for Xconnect.

  Workaround: Remove the Xconnect configuration from the affected VC and then reconfigure it on the VC.

- CSCek70552

  Symptoms: When traffic is directed through a route map that is configured for policy-based routing (PBR) over TE tunnels to a tunnel that is configured for FRR, the traffic may freeze when the protected link flaps.

  Conditions: This symptom is observed on a Cisco 7600 series. When the protected link goes down, traffic does continue through the backup tunnel, but when the protected link returns to normal operation, traffic may freeze.

  Workaround: Detach and re-attach the route map.

- CSCek72661

  Symptoms: SNMP context cannot be properly configured under the address-family IPv4 or IPv6 submode as part of the **vrf definition** *vrf-name* command:

  ```
  vrf definition <vrf-name>
  address-family <address-family name>
  snmp context <context-name>
  ```

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

  Workaround: There is no workaround.

- CSCek73818

  Symptoms: A router may crash when the **echo revision** command is enabled under an MPLS OAM configuration.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2SR but is both platform- and release-independent.

  Workaround: There is no workaround.

- CSCek76212

  Symptoms: A ping over a dot1q interface with 118 + n * 256 byte packets (in which n = 0,1,2...) may not go through.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB with a Route Switch Processor 720 (RSP720) when a packet of the size stated in the Symptoms is received on a dot1q interface and must be software-switched. The symptom is specific to the RSP720.

  Workaround: There is no workaround.

- CSCir01182

  Symptoms: A ping that is issued via the **ping mpls pseudowire** command from one PE router to another PE router may fail.

  Conditions: This symptom is observed on a Cisco router on which a FEC 128 AToM static pseudowire is established when AToM VCCV packets are sent to verify the connectivity between the two PE routers. Note that the static pseudowire functionality works fine.

Workaround: There is no workaround.

- CSCir01449

  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 on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA or Release 12.2(33)SRB when the following conditions are present:

  - The CPU usage is 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: Do not use SSHv2 when the router is very stressed.

- CSCir02111

  Symptoms: Tracebacks and error messages may be generated on a Supervisor Engine 720.

  Conditions: This symptom is observed when the PSD module in a Cisco 7600 series is reset to the AP mode.

  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
```

- 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.

- CSCsb85982

  Symptoms: A router that is configured for AAA may crash because of a bus error and generate the following error message:

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

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB or Release 12.2SRB and that has AAA authentication enabled.

  Workaround: There is no workaround.

- 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.

- CSCsc22043

  Symptoms: The TCL script feature on Cisco IOS routers allows the use of CLI commands to be issued and the response to be checked for certain matching conditions. When using the TCL script with the **cli_open** command, a VTY for that script is setup for the exec commands to be issued. The output to the VTY only catches (with the **cli_read** and **cli_read_pattern** commands) output which is directly printed out as a result of the command; i.e., allows the script to match the output of the **show interface** command.

Output as the results of debug and syslog cannot be seen by the script. Some test commands on the gateway also uses debug to display the output and this can cause problems trying to monitor for certain conditions.

Conditions: This symptom has been observed by using TCL script to monitor the output of syslog or debug output on the VTY session which the script is using.

Workaround: There is no workaround.

- 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.

- CSCsd73598

  Symptoms: A "%SYS-3-MGDTIMER: Uninitialized timer" error message and traceback may be generated when you remove the **bfd interval** command from a GE-WAN interface

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router. However, the symptom may occur on any platform and with any type of interface when you remove the **bfd interval** command.

  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.

- 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) CSCsi97695

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.

- 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.

- CSCse02510

  Symptoms: On a Cisco router that is configured for Hierarchal Queuing Framework (HQF), the RP may crash and generate an “ALIGN-1-FATAL” error message when the “PC hqf_process_wfq_command” function is accessed.

  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 platforms and releases. The symptom occurs on rare occasions after a service policy has been modified on an ATM subinterface or PVC.

  Workaround: There is no workaround.

- 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.

- 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/12_4t/sec_data_plane_12_4t_book.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.

- 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.

- 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.

- CSCse77758

  Symptoms: The secondary RP may fail to boot (that is, reach the SSO mode) after the **ipv6 unicast-routing** command is disabled on the primary RP. During the reboot of the secondary RP, the following message is displayed on its console:

  ```
  %Cannot disable IPv6 CEF on this platform
  ```

  On the primary RP, the following messages are displayed on its console:

  ```
  Config Sync: Starting lines from PRC file:
  -no ipv6 cef
  ```

  ```
  Config Sync: Bulk-sync failure, Reloading Standby
  ```

  Conditions: This symptom is observed on a Cisco router that has dual RPs and that runs Cisco IOS Release 12.2SB.

  Workaround: First, re-enable IPv6 by entering the **ipv6 unicast-routing** command on the primary RP. Then, reboot the secondary RP.

- CSCse98235

  Symptoms: Hardware-switched multicast traffic may be adversely affected by a subinterface configuration. When a large number of subinterfaces (about 1000) are disables and then enabled by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a physical interface, some of the subinterfaces are missing from the OIF list.

  Conditions: This symptom is observed on a 20-port Ethernet Services line card (7600-ES20-GE) that is installed in a Cisco 7600 series.

  Workaround: Enable the Consistency Checker.

- CSCsf13044

  Symptoms: The outgoing interface (OIF) for bidirectional PIM multicast routes is not updated properly because PIM joins are not received through the MDT tunnel.

  Conditions: This symptom is observed on a Cisco 7600 series that has Gigabit Ethernet interfaces that are configured for dCEF. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

- 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.

- CSCsf98858

  Symptoms: Failure detection time with Bidirectional Forwarding Detection (BFD) echo mode takes longer than with BFD asynchronous mode.

  Conditions: This symptom is observed on a Cisco router that has 100 BFD neighbors.

  Workaround: Use the BFD asynchronous mode by entering the **no bfd echo** command on the interface that has BFD enabled.

- 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.

- 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.

- 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.

- CSCsg37644

  Symptoms: Cisco IOS SLB does not function when the client is located behind the MPLS cloud.

Conditions: This symptom is observed on a Cisco 7600 series when the response packets to the client are forwarded over the MPLS tunnel interface.

Workaround: There is no workaround.

- CSCsg40391

  Symptoms: When a dot1x port is authenticated and assigned a VLAN by an AAA server and then the line card for the port is reset, the assigned VLAN becomes the configured access VLAN for the port. You can see this situation in the running configuration for the port.

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

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, reconfigure the access VLAN for the port to the old value.

  Further Problem Description: If, at a later time, you unconfigure dot1x on the port but do not unconfigure the access VLAN, the configuration for the assigned VLAN remains in place, causing the port to have access to whatever VLAN was previously assigned.

- 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.

- 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)
  ```

- 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)
```

- 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.

- CSCsg51811

  Symptoms: When the OER BGP Inbound Optimization feature is configured and when route control is enforced, route control does not prepend autonomous systems or communities. Rather, router control prepends the same autonomous systems or communities to all external OER interfaces.

  Conditions: This symptom is observed on a Cisco router when OER manages inside prefixes that are either learned or configured.

  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.

- CSCsg62226

  Symptoms: An active HSRP router may crash when you configure and unconfigure Hot Standby Router Protocol (HSRP) multiple times.

  Conditions: This symptom is observed when the active router and the standby router are configured with a single Front Door VRF (FVRF) and a single Inside VRF (IVRF), when routing through a GRE tunnel over a VTI occurs via EIGRP, and when the physical IP connectivity occurs via OSPF.

  Workaround: To prevent the symptom from occurring, do not configure and unconfigure HSRP multiple times, but reload the routers and reconfigure both of them.

- CSCsg64170

  Symptoms: When an SSO switchover occurs for an RSP or supervisor engine, network traffic loss may occur or the active Firewall Services Module (FWSM) may unexpectedly failover to the standby FWSM in an unusual way in that both the active and the standby FWSMs become active (that is, the active FWSM remains active and the standby FWSM becomes active). This situation causes traffic loss to and from the FWSMs until the standby FWSM enters the standby state.

  The symptom is not restricted to the FWSMs but may also occur with the following service modules:

  - WS-SVC-WEBVPN-K9
  - WS-SVC-SSL-1-K9
  - WS-SVC-FWM-1-K9
  - WS-X6066-SLB-APC
  - WS-X6066-SLB-S-K9

  Conditions: These symptoms are observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have service modules installed in slot 1 and slot 2. The symptoms occur when two power supplies are inserted in the chassis but only one power supply is turned on or one power supply fails during normal operation, and then a SSO switchover occurs. The symptoms do not occur when both power supplies are turned on or when there is only one power supply in the chassis.

  Workaround: Ensure that both power supplies are turned on.

  Alternate Workaround: Install the service modules in any slots other than slot 1 or slot 2.

- CSCsg68406

  Symptoms: After a HA switchover occurs because you have entered the **issu runversion** command, a link flap may occur on the uplink ports of the newly active supervisor engine, causing traffic on these ports to be disrupted for several seconds and the following error message to be generated on the console:

  ```
  %EARL-SP-2-SWITCH_BUS_IDLE: Switching bus is idle for 10 seconds. The card grant is 7
  ```

Conditions: This symptom is observed on a Cisco 7600 series that is configured with a certain combination of line cards and occurs only during the Enhanced Fast Software Upgrade (EFSU) process. In particular, the symptom is observed when the router has redundant Supervisor Engine 720 cards, one or more legacy line cards such as a WS-X6148-GE-TX, and one or more EFSU-enabled cards such as a WS-X6724-SFP.

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.

- CSCsg82389

  Symptoms: When a T1 controller is shut down on a 1-port channelized OC-3 STM1 ATM CEoP SPA (SPA-1CHOC3-CE-ATM), the CEM circuit that is attached to the T1 controller remains up. This is not proper behavior: when the T1 is controller is shut down, the CEM circuit should also go down.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when a T1 or T3 controller on a SPA-1CHOC3-CE-ATM is shut down.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command for the individual CEM circuit that is attached to the T1 controller.

- 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.

- CSCsg94565

  Symptoms: An incorrect MTU may be used for a GRE/IPSec tunnel that is configured on an IPSec SPA VPN module (SPA-IPSEC-2G), causing unexpected fragmentation.

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

  Workaround: There is no workaround.

- CSCsg99394

  Symptoms: A Frame Relay map may take a long time to be populated after a line card has reset one of the peers.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for dMFR, that dMFR bundles configured on a SPA that is installed in a SIP-200, and that is connected to another router that is also configured for dMFR.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs because Rx and Tx sequence numbers get out of synchronization between the peers.

- CSCsg99877

  Symptoms: Load-sharing on core links may not function.

  Conditions: This symptom is observed on a Cisco router that functions in an AToM configuration with multiple VCs, with traffic flowing through each VC, and with multiple equal-cost paths to the core.

  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.

- CSCsh02724

  Symptoms: The standby RP crashes continuously, that is, the standby RP is reset continuously.

  Conditions: This symptom is observed when an MTR-aware route processor (RP) is paired with a non-MTR-aware RP in a dual-RP ISSU configuration and when the MTR-aware RP is the active RP.

  Workaround: Ensure that both RPs run an MTR-aware Cisco IOS software image.

- 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.

- CSCsh13291

  Symptoms: When a fatal CEF error occurs on a line card other than the RP, CEF becomes disabled on the RP and therefore on the router.

  Conditions: This symptom is observed on a Cisco router after at least one switchover has occurred since the router booted.

  Workaround: There is no workaround.

  Further Problem Description: Another issue can trigger the symptoms: When two 7600-SSC-400 line cards are present in a Cisco 7600 series, CEF on the active RP disables itself about 100 minutes after the router has booted if one or more switchovers have occurred during these 100 minutes.

- 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 is 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.

- CSCsh18070

  Symptoms: Routing protocols may flap on a service instance or routed VPLS (R-VPLS) interface.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured with an Ethernet Services (ES20) line card and any WAN module and/or SIP. The symptom occurs when the traffic through the service instance or R-VPLS interface exceeds the line rate in the egress direction or when the traffic exceeds the shape rate in the class-default class of an MQC policy.

  Workaround: There is no workaround. The symptom is less likely to occur when you reduce the traffic on the port to below the line rate or below the shaping rate.

  Further Problem Description: The symptom occurs because control packets are not treated as high-priority packets on the service instance or R-VPLS interface.

- 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.

- CSCsh20479

  Symptoms: IP services that are configured on an active software EoMPLS VC may not process L3 control frames.

  Conditions: This symptom is observed on a Cisco router when an active software EoMPLS VC (that is, when an Xconnect statement is configured via an SVI/VLAN interface) is configured with an L3 IP address and L3 control frames such as L3 ARP or OSPF multicast frames.

  Workaround: Remove the SVI interface and recreate the SVI interface with the L3 IP address before you configure the EoMPLS xconnect statement. Doing so enables IP services first and then the EoMPLS VC, allowing both to function properly.

- CSCsh21398

  Symptoms: A Cisco 7600 series in which a WS-F6700-DFC3BXL module with 256 MB of memory is installed may run out of memory and display memory allocation failure messages such as the following:

  ```
  %SYS-DFC2-2-MALLOCFAIL: Memory allocation of 4188 bytes failed from 0x205336A0,
  alignment 0 Pool: Processor  Free: 56780  Cause: Memory fragmentation

  Alternate Pool: None  Free: 0  Cause: No Alternate pool

  -Process= "XDR LC Background", ipl= 0, pid= 181

  -Traceback= 20412DD8 2041331C 2050227C 2050BD08 205336A8 211642AC 2113B39C 211393B4
  2114C100 2114ADBC 2113721C 21137354 2113794C 21137CE8 211B7C78 21202F10

  %FIB-2-FIBDISABLE: Fatal error, slot 2/0 (2): CEF-Common: no memory

  %ADJ-DFC2-3-ALLOCATEFAIL: Failed to allocate an adjacency

  -Traceback= 20412DD8 2041331C 211A3DE0 211A4414 21129664 21129850 21139294

  211393A4 2114C100 2114ADBC 21e1 3t7o2 1aC  f2a1tal err1or.37354 2113794C 21137CE8
  211B7C78 21202F10

  %COMMON_FIB-DFC2-3-NOMEM: Memory allocation failure for path list in Common

  CEF [0x21139490] (fatal) (0 subsequent failures).

  %COMMON_FIB-DFC2-4-DISABLING: Common CEF is being disabled due to a fatal error.

  %FIB-2-FIBDISABLE: Fatal error, slot 2/0 (2): CEF-Common: no memory

  %XDR-DFC2-6-XDRLCDISABLEREQUEST: Client CEF push requested to be disabled.

  -Traceback= 20412DD8 2041331C 21217E98 211B0C48 211B3760 21155594 21159FF4 21153D4C
  21153F10 204F6448 204F6434

  %COMMON_FIB-DFC2-4-DISABLING: Common CEF is being disabled due to a fatal error.
  ```

  Conditions: This symptom is observed in a scaled configuration (which is typical of broadband deployments) when 28,000 access subinterfaces are created and brought up.

  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.

- CSCsh34536

  Symptoms: A Circuit Emulation (CEM) group configuration may become lost on the standby RP.

  Conditions: This symptom is observed on a Cisco 7600 series when you perform the following steps:

  1. You configure a CEM interface and groups on a Circuit Emulation over Packet (CEoP) SPA.
  2. You shut down the SPA.
  3. You reload the standby supervisor engine and wait until it comes up.
  4. You bring up the SPA from the active RP.

  At this point, the CEM group configuration is lost on the standby RP.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the standby supervisor engine once more.

- CSCsh35236

  Symptoms: A 20-port Ethernet Services line card (7600-ES20-GE) may crash and a "mac_xid=0x10000" PXF exception may be generated.

  Conditions: This symptom is observed on a Cisco 7600 series under a rare condition when a specific (test) source MAC address triggers the crash and when the router function under stress.

  Workaround: There is no workaround.

- CSCsh35451

  Symptoms: In an HA configuration when the router is in the runversion-switchover state, when you enter the **issu runversion** command, the newly active supervisor engine does not come up fully and causes the standby supervisor engine to crash with "Active_Not_Responding" error messages.

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

  1. You enter the **issu loadversion** command, and you wait for the router to enter the terminal state.
  2. You enter the **issu runversion** command, and you wait for the router to enter the terminal state.

3. The active supervisor engine crashes, and then moves to the RunVersionSwitchOver (RVSO) state.
4. The newly active RP and standby RP come up, and you wait for the router to enter the terminal state.
5. Again, you enter the **issu runversion** command on the active supervisor engine.

At this point, the symptom occurs.

Workaround: There is no workaround.

- CSCsh37272

  This caveat consists of three symptoms, three conditions, and one general workaround:

  Symptom 1: "Invalid element for addition!" syslog messages may be generated.

  Condition 1: This symptom is observed in any BFD configuration.

  Symptom 2: The CPU usage may increase unexpectedly to 99 percent for 30 seconds.

  Condition 2: This symptom is observed on a Cisco 7600 series that has a Route Switch Processor 720 (RSP 720) and that is configured for BFD.

  Symptom 3: The router may reload unexpectedly.

  Condition 3: This symptom is observed on a Cisco 7600 series that is configured with a SIP-400 in which a SPA-2X1GE is installed on which there are many subinterfaces, most of which have the **no bfd echo** command enabled.

  Workaround: There is no workaround.

- CSCsh40540

  Symptoms: When a service instance is configured for Xconnect, the pseudowire fails to come up, and an "%SW_MGR-SP-3-CM_ERR" error message is displayed.

  Conditions: The symptom is observed on a Cisco 7600 series only when encapsulation is configured as default.

  Workaround: There is no workaround.

- CSCsh40567

  Symptoms: When OAM cells are transported over a local-switched connection that is configured for AAL5 and for which the VPI or VCI do not match at both endpoints, OAM cells are dropped.

  Conditions: This symptom is observed on a Cisco 7600 series on an ATM SPA that is installed in a SIP-200 or on an ATM port adapter that is installed in a FlexWAN or Enhanced FlexWAN module.

  Workaround: Ensure that the VPI or VCI are the same at both endpoints of the local-switched connection.

- CSCsh42857

  Symptoms: After a TE tunnel has been reoptimized, AToM traffic may no longer pass through because the outgoing label and outgoing interface are not updated in the hardware.

  Conditions: This symptom is observed on a Cisco 7600 series that has AToM circuits configured over a TE tunnel that connects to a CE router.

  Temporary Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the interface that faces the CE router or configure and deconfigure the **xconnect** command on the interface that faces the CE router. Doing so re-establishes traffic forwarding until a new reoptimization occurs.

- CSCsh45829

  Symptoms: An interface that is configured for Xconnect fails to come up.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a Supervisor Engine 32 and that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCsh45905

  Symptoms: A newly active SP may not be set up correctly with the required Xconnect session information for any of the configured Xconnect sessions.

  Conditions: This symptom is observed when you initiate an HA switchover on a Cisco 7600 series that functions as a PE router and that has a large number of Xconnect sessions configured.

  Workaround: There is no workaround.

- CSCsh47823

  Symptoms: CPU usage may become very high. When this situation occurs, a line card may become unable to respond to keepalive polling from the supervisor engine, and the Switch Processor (SP) may reset the line card.

  Conditions: This symptom is observed on a Cisco 7600 series that has a scaled QoS configuration when the Route Processor (RP) sends many configuration changes to the line card.

  Workaround: On both the RP and the SP, disable resetting of the line card for keepalive response failures. On the RP, enter the **test scp linecard keepalive disable** command; on the SP, enter the **debug oir no-reset-on-crash** *slot* command.

- 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.

- CSCsh57212

  Symptoms: After you have entered the **issu runversion** command, the policy counters in the output of the **show policy-map** command may be zero.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for QoS.

  Workaround: Remove and re-apply the policy.

- CSCsh58337

  Symptoms: After a SSO switchover has occurred, a service policy does not function properly.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that has a service policy that is attached to a CEM circuit.

  Workaround: After the SSO switchover has occurred, reload the SPA on which the CEM circuit is configured by performing a soft OIR.

- CSCsh59439

  Symptoms: You may not be able to configure the same HSRP virtual MAC address on several interfaces or subinterfaces of the same router. When you attempt to do so, the following error message is generated:

  ```
  % MAC address already specified on another group on a different interface.
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for HSRP and is not release-specific.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.4.

- CSCsh59650

  Symptoms: After you have performed an OIR of an Ethernet Services (ES20) line card that has EFP or EVC service instances configured, control plane information may not be re-downloaded onto the line card. This situation prevents data-plane traffic from being passed, even though the RP does not generate any error messages.

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

  Workaround: Reload the line card by entering the **hw-module module** *slot-number* **reset** command.

- CSCsh61393

  Symptoms: When the standby supervisor engine becomes active after an RPR+ switchover has occurred, the transmission of all traffic stops.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in an EoMPLS environment. The symptom occurs because a VRF-VLAN with an explicit null label is not properly programmed on the SP and DFC after the standby supervisor engine has become active. This situation can be seen in the output of the following commands:

  On the RP:

Enter the **show mls cef mpls detail labels** *value* command. For the *value* argument, enter the VRF-VLAN with the explicit null label.

On the SP:

- Enter the **show mls cef mpls detail labels** *value* command. For the *value* argument, enter the VRF-VLAN with the explicit null label.
- Then, enter the **show mls cef adjacency entry** *index* command. For the *index* argument, enter the adjacency index shown in the output of the **show mls cef mpls detail labels** *value* command.

Workaround: There is no workaround.

- CSCsh61851

  Symptoms: A PIM neighborship does not come up on an MDT tunnel when VRFs are removed and added back immediately on PE routers.

  Conditions: This symptom is observed on Cisco 7600 series routers that run Cisco IOS Release 12.2(33)SRB.

  Workaround: Wait for 3 to 4 minutes after you have removed the VRFs on the PE routers so that the backbone entries that are associated with the VRFs expire. Then, add back the VRFs.

  Further Problem Description: The VPN ID is not re-used when a VRF is removed and recreated. This situation results in stale VPN information on the supervisor engine and DFC because backbone entries that are associated with the old VRF can exist until they expire. When a new VPN ID is issued because you recreate the VRF, the hardware entry may not be programmed correctly because of the stale VPN information, preventing the PIM neighborship from being established over the MDT tunnel.

- 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.

- CSCsh66675

  Symptoms: When Circuit Emulation circuits are configured in a very short period via a script and then an RPR+ switchover occurs, the interface of a Circuit Emulation over Packet (CEoP) SPA may shut down.

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

Workaround: After the RPR+ switchover has occurred, enter the **no shutdown** interface configuration command on the interface of the CEoP SPA.

- CSCsh66793

  Symptoms: After you have performed an OIR of a line card, the number of queues that correspond to QoS policies are smaller than before the OIR because not all queues are recreated.

  Conditions: This symptom is observed on a Cisco 7600 series that has a large number of Ethernet Virtual Circuit (EVC) instances on which QoS policies are configured and that are spread across several interfaces.

  Workaround: Perform another OIR of the line card.

- CSCsh73935

  Symptoms: A router may reload when you perform an snmpwalk on the ciscoMvpnMrouteMdtTable.

  Conditions: This symptom is observed when all of the following conditions are present:

  – IP multicast routing is enabled on a VPN routing/forwarding instance (VRF)
  – This VRF is associated with an interface.
  – The Multicast Distribution Tree (MDT) default group address is not configured for the VRF.

  Workaround: Configure the MDT default group address for the VRF by entering the **mdt default** *mdt group* command in VRF configuration mode.

- CSCsh73972

  Symptoms: Traffic that arrives on an interface of a SIP-600 and that should be forwarded over a GRE tunnel with tunnel protection as encrypted packets may be sent unencrypted.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that contain a SIP-600 in one slot and a Services SPA carrier card in which an IPSec VPN SPA (SPA-IPSEC-2G) is installed in another slot.

  Workaround: There is no workaround.

- CSCsh75001

  Symptoms: After a SIP-400 or the router reloads, interfaces remain down until you enter the **shutdown** command followed by the **no shutdown** command on the affected interfaces.

  Conditions: This symptom is observed on a Cisco 7600 series that has a SIP- 400 in which the following SPAs are installed:

  – a 2-port GE SPA (SPA-2X1GE)
  – a 1-port channelized OC-3 STM1 ATM CEoP SPA (SPA-1CHOC3-CE-ATM)

  The interfaces of these SPA are configured with more than 3000 Ethernet Virtual Connection (EVC) flexible instances that are configured for QoS.

  Workaround: There is no workaround.

  Further Problem Description: Configuring more than 3000 EVC instances with QoS on a SIP-400 in which both a SPA-2X1GE and a SPA-1CHOC3-CE-ATM are installed is not supported. A large configuration of EVC instances with QoS can be achieved only without a SPA-1CHOC3-CE-ATM in the SIP-400 in which the SPA-2X1GE is installed.

- CSCsh75176

  Symptoms: A standby RP with a VRF configuration may reload continuously.

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

Workaround: There is no workaround.

- CSCsh75609

  Symptoms: When you enter the **show class cem detail** command, the RP of a Cisco 7600 series may crash because of a TLB exception.

  Conditions: This symptom is observed when the CEM class group is defined by and associated to CEM circuits that are shown in the output of the **show class cem detail** command.

  Workaround: There is no workaround.

- CSCsh75730

  Symptoms: Explicit Congestion Notification (ECN) does not function when ECN-capable Transport (ECT) or CE bits are set to 1.

  Conditions: This symptom is observed on a Cisco router that is configured for QoS and that sends traffic.

  Workaround: There is no workaround.

- 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.

- CSCsh83467

  Symptoms: A standby Supervisor Engine 720 may reset when an entire Circuit Emulation (CEM) configuration is removed and then reconfigured.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when the **recovered-clock** command is present in the removed configuration.

  Workaround: Do not remove an entire CEM configuration.

  Alternate Workaround: Disable the **recovered-clock** command before you remove and then reconfigure an entire CEM configuration.

- 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.

- CSCsh90556

  Symptoms: Traffic may fail to match the VLAN TCAM, causing traffic to be dropped from a SPA that is installed in a SIP-400.

  Conditions: This symptom is observed on a Cisco 7600 series when an Xconnect service is configured and when double-tagged frames are sent via a service instance that is configured with single-tag encapsulation.

Workaround: Configure two service instances, as in the following examples:

  - A service instance to handle single-tagged packets with VLAN ID = 100:

    service instance *10* **ethernet**

    encapsulation dot1q *100*

  - A service instance to handle double-tagged packets with the outer tag = 100:

    service instance *20* **ethernet**

    encapsulation dot1q *100* **second-dot1q** *any*

- CSCsh90762

  Symptoms: The hardware adjacencies that correspond to 6PE aggregate labels may be wrongly programmed.

  Conditions: This symptom is observed on a Cisco 7600 series that functions as a 6PE router.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interfaces that are associated with the IPv6 prefixes that correspond to the affected 6PE aggregate labels.

- CSCsh92709

  Symptoms: The output of the **show users** command may display the wrong mode of the connection with the user. For example, a PPPoE connection may be shown as a PPPoX25 connection.

  Conditions: This symptom is observed on a Cisco router that is configured with a virtual-template interface.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsi04396

  Symptoms: Dynamically changing the **rewrite ingress tag** command for an Ethernet virtual circuit (EVC) service instance may not work.

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

  Workaround: Remove the service instance and re-add it with the new tag manipulation that is to be performed on the frame ingress to the service instance.

- 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.

- CSCsi10458

  Symptoms: A SIP-200 may unexpectedly reset and generate “SIP-1-PAUSE” error messages.

  Conditions: This symptom is observed when large BGP updates occur simultaneously with IPC/EOBC problems.

  Workaround: There is no workaround.

- 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.

- CSCsi15821

  Symptoms: When an SSO switchover occurs after you have enabled and disabled the **mls mpls recir-agg** command or removed the recirculated aggregated labels, the newly active supervisor engine may not place the aggregate labels in VPN CAM.

  Conditions: This symptom is observed on a Cisco 7600 series when the total number of aggregate labels that is created is greater than the maximum number of aggregate labels that can be placed in the VPN CAM.

Workaround: There is no workaround.

- CSCsi22291

  Symptoms: A SIP-200 may unexpectedly reset and generate “SIP-1-PAUSE” error messages.

  Conditions: This symptom is observed when large BGP updates occur simultaneously with IPC/EOBC problems.

  Workaround: There is no workaround.

- CSCsi25583

  Symptoms: The standby supervisor engine may reset continuously and the following messages are generated in the log:

```
Config Sync: Starting lines from MCL file:
controller E1 2/0/0
! <submode> "controller"
- framing UNFRAMED
! </submode> "controller"
controller E1 2/0/2
! <submode> "controller"
- framing UNFRAMED
! </submode> "controller"
```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a SPA-8XCHT1/E1 and occurs only when the controller functions in unframed mode.

  Workaround: There is no workaround.

- 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 in Release 12.2(28)SB5.

- CSCsi29423

  Symptoms: Unable to ping when packet verification is turned on.

  Conditions: This symptom occurs when packets are corrupted at tail part.

  Workaround: There is no workaround.

- CSCsi35931

  Symptoms: Traffic is dropped when it traverses an EoMPLS pseudowire that is configured for Xconnect on an interface of a SIP-400.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that has a Supervisor Engine 720. The symptom occurs when a packet leaves one side of the layer 2 network with a payload of 1500 bytes and is destined for the SIP-400 side of the pseudowire. The packet is dropped before it arrives at the SIP-400.

Workaround: When traffic must traverse an EoMPLS pseudowire that is configured for Xconnect, do not use a SIP-400 to terminate this connection. Rather, use another card. A possible workaround may be to change the MTU of the interface of the SIP-400 to 1522 bytes.

- CSCsi64093

  Symptoms: When an Ethernet Services (ES20) line card functions in a VPLS or Multipoint Bridging (MPB) configuration and faces the core, half of the imposition traffic may be dropped in the core.

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

  The symptom occurs in a VPLS or MPB configuration when, for core-facing packets, the address of the imposition router is used as the source MAC address. In this situation, the upper 16 bits of this address is corrupted with either 0 or 0xFFFF. Some core routers and switches may drop packets with 0xFFFF address corruption, which can be verified by looking at the core-facing source MAC addresses with a sniffer. Because of the distribution of 0 and 0xFFFF source MAC addresses, the amount of dropped packets may be approximately 50 percent of the imposition traffic.

  Workaround: There is no workaround.

- CSCsi71285

  Symptoms: An SNMP walk of VLAN statistics or executing the **show vlan counters** command causes the console to wait indefinitely or causes a CPUHOG condition.

  Conditions: This symptom is observed only on a Cisco 7600 series that runs Cisco IOS Release 12.2SRA when VLAN statistics are collected from cached entries.

  Workaround: Do not collect VLAN statistics from cached entries. Rather, ensure that VLAN statistics are collected real-time.

  Further Problem Description: Both SNMP queries and CLI commands block while retrieving non-routed VLAN counters. An SNMP query on any of the ifTable counters for a non-routed VLAN interface blocks the SNMP agent indefinitely. This situation causes the SNMP AGENT queue to fill up and, consequently, SNMP packets to be dropped. In turn, this situation prevents the Network Management application from accessing any other MIB objects that are not related to the non-routed VLANs. Restarting the SNMP agent clears the thread, but as soon as another objects related to the non-routed VLAN is accessed, the SNMP agent blocks again.

- CSCsi99825

  Symptoms: An SNMP Engine may crash at the “idb_get_swsb” and “mpls_if_get_gen_stats” functions.

  Conditions: This symptom is observed on a Cisco 7613 that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: Disable this SNMP query from the CU.

- 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

- 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

- 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).

- CSCsi43652

  Symptoms: A Cisco 7600 series that is configured for In Service Software Upgrade (ISSU) may not initialize the standby RP.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for SSO when the active RP runs Cisco IOS Release 12.2(33)SRB or an earlier release and when the standby RP runs Release 12.2(28)SB or a later release.

  Workaround: Do not configure SSO. Rather, configure RPR or RPR+.

Open Caveats—Cisco IOS Release 12.2(33)SRB

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(33)SRB. All the caveats listed in this section are open in Cisco IOS Release 12.2(33)SRB. This section describes only severity 1, severity 2, and select severity 3 caveats.

Interfaces and Bridging

- CSCsf20174

  Symptoms: An enhanced FlexWAN module may reload with certain traffic flows.

  Conditions: This symptom is observed rather rarely on a Cisco 7600 when the enhanced FlexWAN module is configured with an ATM port adapter, has 1483 configurations, and processes traffic.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCek34591

  Symptoms: In a scaled MTR configuration, a memory leak may occur and the memory may be depleted.

  Conditions: This symptom is observed on a Cisco router when you remove the BGP process or when BGP prefixes are advertised or withdrawn.

  Workaround: There is no workaround.

- CSCek69784

  Symptoms: The **redistribute static route-map** command may not function as expected.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured for BGP.

  Workaround: There is no workaround.

- 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.

- CSCsc26247

  Symptoms: Conflicts may occur between the routes in a BGP table and an IP routing table.

  Conditions: This symptom is observed on a Cisco router when BGP routes that are learned via multipaths are reported as locally generated routes (0.0.0.0) in the IP routing table.

  Workaround: There is no workaround.

- CSCsd27372

  Symptoms: BGP may not converge in the specified time and the CPU usage may be near 99 percent.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for VPN and BGP and that functions in a large-scale configuration.

Workaround: There is no workaround.

- CSCsh02161

  Symptoms: A Route Reflector (RR) does not withdraw a prefix that redistributes itself even if this prefix is removed from the BGP table.

  Conditions: This symptom is observed on a Cisco router that functions as an RR that advertises two of the same prefixes with different Route Distinguishers (RDs) when one of these prefixes redistributes itself and when the other prefix is a route that is learned from an RR client via iBGP.

  Workaround: There is no workaround.

- CSCsh12384

  Symptoms: Removing a loopback interface when RSVP sessions are active causes a traceback.

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

  Workaround: There is no workaround. However, there is no functional impact to the router.

- CSCsh32655

  Symptoms: A router may crash when you remove a configuration that consists of multiple instances of BGP and the **ip access-list** command.

  Conditions: This symptom is observed on a Cisco router when you remove the configuration through a TFTP server.

  Workaround: Do not use a TFTP server to remove a BGP configuration.

- CSCsh58933

  Symptoms: Route convergence for MPLS VPN routes is slower than expected.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured for BGP when the MPLS VPN routes are received by another router that functions as a provided edge (PE) router.

  Workaround: There is no workaround.

- CSCsh64985

  Symptoms: After a switchover occurs on a remote PE router, a tunnel interface that has the **ip pim vrf** *vrf-name* **rp-address** command enabled cannot be found on the local PE router.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router, that is configured for MVPN, and that functions in a provider core network.

  Workaround: There is no workaround.

- CSCsh73139

  Symptoms: IPv6 routes that are redistributed via the **redistribute connected** address family configuration command may disappear after you have performed an OIR of an Enhanced FlexWAN line card.

  Conditions: This symptom is observed on a Cisco 7600 series. Note that only IPv6 is affected, IPv4 works fine.

  Workaround: Disable and then re-enable the **redistribute connected** address family configuration command.

- CSCsh78416

  Symptoms: Stale routes are not flushed from the routing table after the stale path timer has expired during a graceful restart of a BGP session. As a result, all unwanted traffic continues to be processed by the router for those stale routes.

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured for BGP graceful restart. The symptom occurs when, during the graceful restart of the BGP session, a non-established active session resets.

Workaround: Clear or restart the BGP process on the router to remove all stale routes.

- CSCsh78786

  Symptoms: When you enter the **no address-family ipv4 mdt** command followed by the **address-family ipv4 mdt** command, a Multicast Distribution Tree (MDT) peer may not come up.

  Conditions: This symptom is observed on a Cisco router that functions in a topology with route reflectors and MDT peers.

  Workaround: Enter the **clear ip bgp** *neighbor-address* **ipv4 mdt** command for the affected MDT peer.

- CSCsh79862

  Symptoms: When IP options packets are received at the rate of 1000 pps, excessive BGP and/or OSPF flaps may occur. These flaps stop on automatically after 15 minutes.

  Conditions: This symptom is observed on a Cisco 7600 series while there is a heavy CPU load during the BGP and/or OSPF route reconvergence process.

  Workaround: Enabling a rate limiter for the IP options packets to ensure that the symptom does not occur.

ISO CLNS

- CSCek69976

  Symptoms: An IS-IS adjacency message may not be copied correctly between the active RP and the standby RP.

  Conditions: This symptom is observed on a Cisco router when an In Service Software Upgrade (ISSU) is performed between a Cisco IOS software image with IS-IS ISSU support for adjacency message version 2 and a Cisco IOS software image with IS-IS ISSU support for adjacency message version 4.

  Workaround: There is no workaround.

Miscellaneous

- CSCeh32251

  Symptoms: A mismatched bandwidth may generate corrupt packets that are not detected in the hardware when CRC-16 is configured on the interfaces. The corrupt packets may cause the CPU usage of the RP to increase to 100 percent, and the corrupt packets may be dropped.

  Conditions: This symptom is observed on a Cisco platform that is configured with a 2-port or 4-port clear channel T3/E3 SPA (SPA-2XT3/E3 or SPA-4XT3/E3) or 4-port channelized T3 (DS0) SPA (SPA-4XCT3/DS0) that is configured for T3 DSU Kentrox mode with a subrate bandwidth above 35,000 when the far-end is also configured for DSU Kentrox mode but with a mismatched bandwidth that is less than 35,000

  Workaround: When you use DSU Kentrox mode, configure CRC-32 on the interfaces and configure the correct bandwidth before you enable the interfaces.

- CSCek28110

  Symptoms: XDR tracebacks are generated after an SSO switchover has occurred.

Conditions: This symptom is observed on a Cisco router and seems to occur only after multiple SSO switchovers have occurred.

Workaround: There is no workaround.

- CSCek48810

  Symptoms: The SNMP community still exists after you have entered the following commands:

  ```
  snmp-server comm public rw
  snmp-server comm private rw
  end
  auto secure management no-interact
  ```

  The expected behavior is that the SNMP community is removed after you have entered the **auto secure management no-interact** command.

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

  Workaround: There is no workaround.

- CSCek50234

  Symptoms: The standby RP may reload when you enter the **enrollment url** *url* command on the active RP and when the *url* argument represent any device that is visible on the active RP but not the standby RP. When this situation occurs, the following error messages are generated on the console of the active RP:

  ```
  Config Sync: Bulk-sync failure due to PRC mismatch. Please check the full list of PRC
  failures via:
    show issu config-sync failures prc

  Sync: Starting lines from PRC file:
  crypto pki trustpoint abcd
   ! <submode> "crypto-ca-trustpoint"
  - enrollment url <url> pem
   ! </submode> "crypto-ca-trustpoint"

  Config Sync: Bulk-sync failure, Reloading Standby
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that uses the Public Key Infrastructure (PKI) for authorization. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCek50806

  Symptoms: The standby RP may reload when you enter the **aps revert** command.

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

  Workaround: There is no workaround.

- CSCek53704

  Symptoms: When you first configure and attach more than 255 class maps in a single policy to an interface and when you then remove the policy map, the router crashes.

  Conditions: This symptom is observed on a Cisco router and occurs because a maximum of 255 class maps (that is, 254 user-defined class maps and one default class map) are supported in a single policy map.

Workaround: There is no workaround. Ensure that you do not configure more than 255 class maps, including the default class map, in a single policy map.

- CSCek61489

  Symptoms: An OSM-2+4GE-WAN+ module may reload unexpectedly because of memory corruption.

  Conditions: This symptom is observed on a Cisco 7600 series when an RPR+ switchover occurs or when you first attach an Input VLAN with a policy map with 250 class maps via the **match input vlan** command to an interface and then detach this Input VLAN from the interface.

  Workaround: There is no workaround.

- CSCek63459

  Symptoms: When you enter the **ping mpls traffic-eng tunnel 1 ttl 1** command, a Cisco 7600 series may crash in the "ldap_explode_dns()" process.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured for LDAP.

  Workaround: There is no workaround.

- CSCek63548

  Symptoms: Weighted Random Early Detection (WRED) may not function properly when it is configured at the first level and when a policer is configured at the first and second level over Frame Relay, ATM, or HDLC interfaces.

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

  Workaround: There is no workaround.

- CSCek64619

  Symptoms: The APS manual trigger information may become lost in the k1k2 bytes after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco 7600 series that has a scaled configuration on a 1-port channelized OC-3/STM-1 SPA. The symptom occurs when you first force the working channel to the protect channel by entering the **aps force** command and then an SSO switchover occurs. In this situation, the k1k2 bytes may be reset.

  Workaround: Enter the **aps force** command once more.

  Further Problem Description: This symptom may become problematic when a Add-Drop Multiplexer (ADM) is present and when the channel states are not synchronized in relation to the ADM.

- CSCek64634

  Symptoms: A spurious memory access may be generated at the "memcpy" process during an SSO switchover. The traceback and decode shows the following information:

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router and occurs when the FIB IDB of a virtual interface does not properly synchronize after the SSO switchover has occurred.

  Workaround: There is no workaround.

- CSCek65003

  Symptoms: When you send multicast traffic through a GRE/IPsec tunnel, the output of the **show interface status** command does not show the correct count for outgoing packets. (Note that the counter for incoming packets functions correctly.)

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.

- CSCek65211

  Symptoms: An IPsec VPN SPA may crash when multicast traffic with large packet sizes (incrementing from 5000 to 6000 bytes) is sent at a rate of 10 pps through a GRE tunnel with 50 replications.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with an IPsec VPN SPA and occurs only when the IPsec VPN SPA has interface VLANs with different MTUs, causing the GRE tunnels to adapt these different MTUs. When the interface VLANs have identical VLANs, the GRE tunnels function with the same MTU, and the symptom does not occur.

  Workaround: Configure the same MTU on all interface VLANs.

- CSCek65259

  Symptoms: When multicast packets are fragmented, GRE packets are not encapsulated by a crypto card, even though the **show crypto vlan** command shows that the tunnel is accelerated by the crypto card.

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

  Workaround: Ensure that the GRE packet sizes are smaller than the MTU to enable the crypto card to perform encapsulation.

- CSCek66092

  Symptoms: An IPv6 demultiplexer configuration is rejected over an Ethernet interface when there is an IP address configured on the same interface.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(33)SRB or a release later than Release 12.2(31)SB and that is configured for Xconnect.

  Workaround: There is no workaround.

  Further Problem Description: The following example shows a configuration in which the symptom occurs:

  ```
  router(config)#interface FastEthernet5/0
  router(config-if)#ip address 10.10.10.10 255.255.255.0
  router(config-if)#xconnect 192.168.200.200 100 pw-class ipv6_demux
  Incompatible with ip address command on Fa5/0 - command rejected.
  ```

- CSCek66731

  Symptoms: On a Cisco 7600 series packets that are received by a routed interface that does not have an IPv4 address may be forwarded by CEF.

  Conditions: This symptom is observed when the Cisco 7600 series receives an IP packet on an interface that has no IPv4 address enabled but that has a matching route entry to forward the packet to a destination.

  Workaround: Shut down the interface that has no IPv4 address enabled.

- CSCek67814

  Symptoms: The *bandwidth* argument of the **ip rtp priority** *starting-rtp-port-number port-number-range bandwidth* interface configuration command does not appear when you enter the **show running-config** command.

The same situation may occur for the **ip rtp reserve** *lowest-udp-port range-of-ports [maximum-bandwidth]* command.

The rest of the command is correctly displayed and the bandwidth value that is stored internally is correctly set at 0.

Conditions: This symptom is observed when the *bandwidth* argument (or *maximum-bandwidth* argument) is configured as 0. If any other valid value is configured, it will correctly appear in the output of the **show running-config** command.

Workaround: There is no workaround.

- CSCek68156

  The following caveat has been closed because a crypto connection is supported only on a Gigabit Ethernet subinterface of an IPsec VPN SPA (SPA-IPSEC-2G).

  Symptoms: A crypto connection does not function when you attempt to establish one on a Gigabit Ethernet subinterface of a line card or module other than a SPA-IPSEC-2G.

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

  Workaround: There is no workaround.

- CSCek68370

  Symptoms: An Xconnect interface that is configured on an Ethernet Virtual Circuit (EVC) may remain down.

  Conditions: This symptom is observed when the encapsulation is set to default or untagged.

  Workaround: There is no workaround.

- CSCek68378

  Symptoms: CEF may be unexpectedly disabled after the router has booted or when CEF entries are added at a high rate to an Ethernet module that functions in conjunction with a DFC. When this situation occurs, the output of the **show ip cef** command displays an "%IPv4 CEF not running" message.

  Conditions: This symptom is observed on a Cisco 7600 series that has a Supervisor Engine 720, that runs Cisco IOS Release 12.2(33)SRA2, and that has an Ethernet module such as a WS-X6816-GBIC module that functions in conjunction with a DFC.

  Workaround: There is no workaround.

- CSCek68511

  Symptoms: Packets that match a policy map are shown as zero in the output of the **show policy-map interface** command.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that processes unicast traffic.

  Workaround: There is no workaround.

- CSCek68959

  Symptoms: When a second RPR+ switchover occurs and when an OSM-2+4GE-WAN+ module resets during the switchover, the running configuration may become lost on the OSM-2+4GE-WAN+ module. When this situation occurs, the interfaces and the L2 and L3 VPNS that are configured on the OSM-2+4GE-WAN+ module do not come up, and traffic that is processed over these interfaces and VPNS becomes lost.

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

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, copy the startup configuration to the running configuration.

- CSCek69063

  Symptoms: L3 control packets may not be properly processed when an IP address is configured on a switch virtual interface (SVI).

  Conditions: This symptom is observed on a Cisco 7600 series when an IP address is configured on an SVI on which an **xconnect** is enabled.

  Workaround: Remove the **xconnect** command from the SVI, add the IP address to the SVI, and then re-add the **xconnect** to the SVI.

- CSCek69280

  Symptoms: When you initiate an SSO switchover after several ISSU transitions have been executed, a SIP-400 may reload unexpectedly. When this situation occurs, the following error message is generated:

  ```
  %OIR-SP-3-PWRCYCLE: Card in module 9, is being power-cycled off (Reset - Module
  Reloaded During Download)
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with redundant Route Switch Processor 720 (RSP720) cards after the following sequence of commands has been executed:

  ```
  issu loadversion
  issu abortversion
  redundancy force-switchover
  ```

  or the following sequence of commands:

  ```
  issu loadversion
  issu runversion
  issu acceptversion
  issu abortversion
  redundancy force-switchover
  ```

  Workaround: Do not use the **issu abortversion** command.

  Further Problem Description: The SIP-400 does not normally reload when the **redundancy force-switchover** command is executed. The SIP-400 reloads only if first a sequence of ISSU transitions is performed, and then the **redundancy force-switchover** command is executed.

- CSCek69498

  Symptoms: When sustained cell rate (SCR) is configured in port mode on an interface that is configured for ATM over MPLS (AToM), a VC may not come up.

  Conditions: This symptom is observed on a Cisco router that has the **mpls l2transport route** command enabled.

  Workaround: Unconfigure and then reconfigure the **mpls l2transport route** command. Doing so enabled the VC to come up.

- CSCek69541

  Symptoms: When a first RPR+ switchover occurs, an OSM-2+4GE-WAN+ module or other OSM may crash at the “hqf_layer_cleanup” function.

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

  Workaround: There is no workaround.

- CSCek69576

  Symptoms: The standby Route Switch Processor 720 (RSP720) may become stuck when it reloads after a switchover has occurred. Eventually, the RSP720 resets and boots fine thereafter. When the symptom occurs, the following error messages are generated:

  ```
  %ONLINE-SP-6-TIMER: Module 8, Proc. 0. Failed to bring online because of timer event
  %PFREDUN-SP-6-ACTIVE: Standby processor removed or reloaded, changing to Simplex
  mode)
  ```

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

  Workaround: There is no workaround.

- CSCek69635

  Symptoms: When you perform an ISSU downgrade after an ISSU upgrade has occurred, a SIP-400 may crash and may not record or save the crashinfo file, and the following error messages may be generated:

  ```
  %OIR-3-CRASH: The module in slot 6 has crashed %OIR-6-REMCARD: Card removed from slot
  6, interfaces disabled
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with redundant Route Switch Processor 720 (RSP720) cards after the following sequence of commands has been executed:

  First, you perform and ISSU upgrade to the new Cisco IOS software image:

  issu loadversion

  issu abortversion

  issu runversion

  issu acceptversion

  issu commitversion

  Then, you perform and ISSU downgrade to the old Cisco IOS software image:

  issu loadversion

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **issu abortversion** command and restart the ISSU downgrade procedure by entering the **issu loadversion** command.

- CSCek69641

  Symptoms: When you perform an ISSU downgrade after an ISSU upgrade has occurred, a 10-Gigabit Ethernet Switching Module (WS-X6704-10GE) may crash, and the following error messages may be generated:

  ```
  SP: PREDNLD_ERRMSG: IPC: Failed to tx image pkt to IPC port Slot 9/0: REDNLD: retry
  queue flush [for 9/0]
  %OIR-SP-6-NOPWRISSU: Card inserted in slot 9 powered down because ISSU is in progress
  %MDR_SM-SP-3-SLOT_NOTIFY_TIMEOUT: Notification timeout on MDR slot state machine 9
  for the local client Last SP MDR client (1) in state SLOT_PREDOWNLOAD
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with redundant Route Switch Processor 720 (RSP720) cards after the following sequence of commands has been executed:

  First, you perform and ISSU upgrade to the new Cisco IOS software image:

  issu loadversion

  issu abortversion

  issu runversion

issu acceptversion

issu commitversion

Then, you perform and ISSU downgrade to the old Cisco IOS software image:

issu loadversion

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **issu abortversion** command and restart the ISSU downgrade procedure by entering the **issu loadversion** command.

- CSCek69770

  Symptoms: When you enter the **context snmp** VRF configuration command, the command is accepted but does not appear in the running configuration.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS 12.2(33)SRB and that is configured for MPLS VPN.

  Workaround: There is no workaround.

- CSCek69798

  Symptoms: A router that is configured for QoS may crash without any clear trigger.

  Conditions: This symptom is observed when you change the redundancy mode from RPR+ to SSO.

  Workaround: There is no workaround.

- CSCek69876

  Symptoms: Explicit bumping values are not shown in the output of the **show atm bundle** command.

  Conditions: This symptom is observed on a Cisco router that functions as a CE router when you enter the **no bump explicit** command for an ATM VC class. In this situation, the output of the **show atm bundle** command should show a null value, which it does not.

  Workaround: There is no workaround.

- CSCek69878

  Symptoms: The connectivity check between two CE router may stop functioning.

  Conditions: This symptom is observed on a Cisco router that functions in an ATM and MPLS configuration when you change the experimental bits on the PVC link between two PE routers that are associated with the CE routers.

  Workaround: There is no workaround.

- CSCsb08994

  Symptoms: The **test ip** command returns an ambiguous command error.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS interim Release 12.4(2.5) or interim Release 12.4(2.2)T and that is configured with an NPE-G1 (revision B) processor. However, not that the symptom is both platform- and release-independent.

  Workaround: There is no workaround.

- CSCsb28210

  Symptoms: When you establish a Telnet connection to the IP address of a virtual server, you are unexpectedly connected to a Server Load Balancing (SLB) device on which the virtual IP address is configured.

  Conditions: This symptom is observed when the virtual server functions in dispatch mode, when a real server in a serverfarm that is associated with the virtual server is down, and when the ARP entry for the real server is marked as incomplete.

Workaround: Clear the ARP table in the SLB device before you establish a connection to the virtual server.

Alternate Workaround: Use ping probes to detect a failure of the real server so you can prevent SLB from assigning connections to the failed real server.

- CSCsb29314

  Symptoms: A ping probe does not function in client NAT mode.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that function in a Server Load Balancing (SLB) configuration.

  Workaround: There is no workaround.

  Further Problem Description: Note that the symptom does not occur in Cisco IOS Release 12.2(18)SXF5.

- CSCse23576

  The following caveat has been closed because the situation that is described is a known issue when there is a configuration with a large number of tunnels.

  Symptoms: When you toggle a configuration by entering the **no crypto engine accelerator** *slot* command followed by the **crypto engine accelerator** *slot* command on an interface or interface range, the CPU usage on the router may spike.

  You can verify this situation in output of the **show processes cpu sorted** command, which will show the process "FM core" as one of the top CPU utilizers.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB that functions in a configuration with a a large number of tunnels.

  Workaround: There is no workaround.

- CSCse28397

  Symptoms: The crashinfo context section is missing some register values in the crashinfo file.

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

  Workaround: There is no workaround.

- CSCse52755

  Symptoms: An ELMI link between a PE router and CE router may remain down.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that functions as a PE router when the following conditions are present:

  - The PE router is configured with a SIP-400 that has a SPA with a Gigabit Ethernet interface that connects to the CE router.
  - The Gigabit Ethernet interface has an Xconnect-based Ethernet Virtual Circuit (EVC) configuration.

  Workaround: On the PE router, enter the **ethernet cfm enable** global configuration command.

  Further Problem Description: The symptom occurs because the ELMI packets that are sent by the CE router and are destined for the PE router are tunneled to a remote side instead of being punted to the RP of the CE router.

- CSCse60827

  Symptoms: An IKE/IPsec session fails when you use a TACACS server.

Conditions: This symptom is observed on a Cisco router when PKI is configured along with AAA, as in the following example:

```
ipsecn-7606a(config)#aaa authorization network <list-name> group tacacs+
ipsecn-7606a(config)#crypto ca trustpoint <trustpoint-name>
ipsecn-7606a(ca-trustpoint)#authorization list <list-name>
ipsecn-7606a(ca-trustpoint)#authorization username subjectname country
ipsecn-7606a(ca-trustpoint)#exit
```

Workaround: There is no workaround. Note that the symptom does not occur when you use a RADIUS server.

- CSCse89100

  Symptoms: Key exchange fails during IKE negotiation at the "IKE_I_MM5" state.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA and occurs only when the router is configured for NAT-T and VRF.

  Workaround: There is no workaround.

- CSCse98235

  Symptoms: Hardware-switched multicast traffic may be adversely affected by a subinterface configuration. When a large number of subinterfaces (about 1000) are disables and then enabled by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a physical interface, some of the subinterfaces are missing from the OIF list.

  Conditions: This symptom is observed on a 20-port Ethernet Services line card (7600-ES20-GE) that is installed in a Cisco 7600 series.

  Workaround: Enable the Consistency Checker.

- CSCsf20714

  Symptoms: A DHCP relay may crash at the "print_unaligned_summary" function while requesting an IP address from a DHCP client.

  Conditions: This symptom is observed on a Cisco router after the bridge group has changed from one group to another.

  Workaround: There is no workaround.

- CSCsg10531

  Symptoms: An "Invalid SPI" error message may be generated and packet loss may occur during an SA rekey.

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

  Workaround: There is no workaround.

- CSCsg17537

  Symptoms: The memory consumption of NetFlow Data Export (NDE) is higher than it should be.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2SX or Release 12.2(33)SRB and that is configured for NetFlow.

  Workaround: There is no workaround.

- CSCsg22169

  Symptoms: Memory consumption of the NetFlow Data Export (NDE) process is high.

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 NDE process consumes about 133 KB for per-protocol queues. The fix for this caveat reduces the memory consumption to a little more than half the original usage.

- CSCsg26096

  Symptoms: When you enter the **hw-module reset** command on a 1-port CHOC-3/CHSTM-1 SPA that is installed in a Cisco 7600 series at the local end, the network clock at the remote end may become out-of-range (OOR), that is, the network clock goes beyond the acceptable limits of pps, without an error message being generated.

  Conditions: This symptom is observed when the Network Clocking feature is configured on the 1-port CHOC-3/CHSTM-1 SPA.

  Workaround: There is no workaround.

- CSCsg37644

  Symptoms: Cisco IOS SLB does not function when the client is located behind the MPLS cloud.

  Conditions: This symptom is observed on a Cisco 7600 series when the response packets to the client are forwarded over the MPLS tunnel interface.

  Workaround: There is no workaround.

- CSCsg40482

  Symptoms: ISDN L2 may remain in the “TEI_ASSIGNED” state.

  Conditions: This symptom is observed on a Cisco router after you have performed a hard OIR of a PA-MC-4T1 port adapter.

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

- 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)
  ```

- CSCsg42753

  Symptoms: Some MPLS TE tunnels may be resignaled on the tunnel headend following an SSO switchover.

  Conditions: This symptom is observed on a Cisco 7600 series that has dual RPs that function in SSO mode when and RSVP Graceful Restart is configured in full mode. The symptom occurs only when there are more than 200 tunnel headends established when the SSO switchover occurs.

  Workaround: There is no workaround.

  Further Problem Description: After the SSO switchover has occurred, the output of the **show ip rsvp high-availability counters** command shows that some LSPs failed recovery:

  ```
  LSPs for which recovery:
    Attempted: 600
    Succeeded: 595
    Failed:    5
  ```

  TE prevents new LSPs from being signaled during the RSVP HA recovery period immediately after the SSO switchover has occurred. For any TE tunnels that fail to recover, traffic that is routed onto those tunnels is dropped. However, the tunnels are resignaled after the RSVP HA recovery period, which may take up to two minutes.

- CSCsg42825

  Symptoms: When you attempt to configure more than 1056 traffic engineering (TE) tunnels, the following error message may be generated:

  ```
  "%ERROR: Standby does not support this command"
  ```

  Conditions: This symptom is observed on a Cisco 7600 series when all tunnels are configured at once via a script or via a copy-and-paste operation of the configuration.

  Workaround: Provide an interval between each 10 tunnels so that the tunnels are not configured all at once.

- 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.

- CSCsg62226

  Symptoms: An active HSRP router may crash when you configure and unconfigure Hot Standby Router Protocol (HSRP) multiple times.

Conditions: This symptom is observed when the active router and the standby router are configured with a single Front Door VRF (FVRF) and a single Inside VRF (IVRF), when routing through a GRE tunnel over a VTI occurs via EIGRP, and when the physical IP connectivity occurs via OSPF.

Workaround: To prevent the symptom from occurring, do not configure and unconfigure HSRP multiple times, but reload the routers and reconfigure both of them.

- CSCsg64557

  Symptoms: The tunnel interface counter does not increment in tunnel protection mode.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with GRE tunnels when an IPsec VPN SPA (SPA-IPSEC-2G) processes the GRE tunnels and when the crypto functionality is configured for tunnel protection mode.

  Workaround: There is no workaround. However, to trace the packet path other interface counters (such as counter on the physical interface or VLAN interface) can be checked.

- CSCsg68406

  Symptoms: After a HA switchover occurs because you have entered the **issu runversion** command, a link flap may occur on the uplink ports of the newly active supervisor engine, causing traffic on these ports to be disrupted for several seconds and the following error message to be generated on the console:

  ```
  %EARL-SP-2-SWITCH_BUS_IDLE: Switching bus is idle for 10 seconds. The card grant is 7
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a certain combination of line cards and occurs only during the Enhanced Fast Software Upgrade (EFSU) process. In particular, the symptom is observed when the router has redundant Supervisor Engine 720 cards, one or more legacy line cards such as a WS-X6148-GE-TX, and one or more EFSU-enabled cards such as a WS-X6724-SFP.

  Workaround: There is no workaround.

- CSCsg78244

  Symptoms: You can still ping a Server Load Balancing (SLB) virtual IP (VIP) address after all of the real server in the serverfarm fail.

  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: One example in which the symptom occurs is the following:

  When there is a redundant configuration of two SLBs devices with similar configurations and when the real servers that are bound to a virtual server in the primary connection fail, the secondary SLB device handles the connections. Even when the real servers that are bound to the virtual server in the primary SLB connection fail, you can still ping the VIP, which means that the virtual server is still in service. This situation causes traffic to continue to be routed to the VIP on the primary SLB device.

- CSCsg79129

  Symptoms: Multicast traffic may not be forwarded on a routed VPLS (R-VPLS) interface that is configured for PIM Sparse Mode (SM).

  Conditions: This symptom is observed on a Cisco 7600 series that has a SIP-600 on which an RPF interface is configured and occur when egress replication mode is enabled.

  Workaround: Change the multicast replication mode from egress mode to ingress mode by entering the **mls ip multicast replication-mode ingress** command.

- CSCsg84374

  Symptoms: CPUHOG messages may be generated on the console of the RP when you run the cbQosPoliceCfg MIB object of the Cisco Class-Based QoS MIB.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in a scaled configuration.

  Workaround: There is no workaround.

- CSCsg84522

  Symptoms: A router may crash because of ATM Inverse ARP (InARP) timer issues.

  Conditions: This symptom is observed on a Cisco router when you configure or deconfigure the InARP timer.

  Workaround: There is no workaround.

- CSCsg87290

  Symptoms: When you enter the **shutdown** command followed by the **no shutdown** command on the SONET controller of a 1-port channelized STM1/OC3 to DS0 SPA (SPA-1XCHSTM1/OC3), an extra flap occurs for T3 links that are configured on the SONET controller.

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

  Workaround: There is no workaround.

- CSCsg98041

  Symptoms: The TCP checksum is incorrect when both NAT-T and transport mode are configured.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB for TCP sessions that are terminated on the router.

  Workaround: Do not use transport ode. Rather, use tunnel mode.

  Alternate Workaround: Configure GRE keepalives on termination point (TP) tunnels to protect TCP traffic that is destined for the router.

- CSCsh02510

  Symptoms: A router crashes when you configure an Xconnect service on a main interface.

  Conditions: This symptom is observed on a Cisco router that has two or more L2VPN connections that are configured for Xconnect service on a subinterface of the main interface. Even after you have deleted the subinterface, the router crashes when you configure Xconnect service on the main interface.

  Workaround: There is no workaround.

  Further Problem Description: This symptom was initially observed on a Cisco 10000 series when you configured Xconnect service on a main interface of a 6-port channelized T3 line card or 4-port channelized STM-1/OC-3 line card. However, the symptom appeared to be platform-independent.

- CSCsh12653

  Symptoms: When an ISG receives VSAs that cannot be parsed by the SIP parser, the ISG disconnects the established session and does not respond with a CoA Nak message.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG when an incorrect VSA is sent via a CoA message and when the SIP parser returns a DENY message to the ISG.

Following are examples of incorrect VSAs:

- a vc-weight that is larger than the maximum that is allowed:
  cisco-avpair = “atm:vc-weight=3000”
- a non-existent service-policy name:
  cisco-avpair = “atm:vc-qos-policy-out=non_exist_policy”
  cisco-avpair = “atm:vc-watermark-max=1”

Workaround: There is no workaround.

- CSCsh16387

  Symptoms: When the default ACL of an interface is configured as a software bridge, all traffic that enters this interface is punted to the RP.

  Conditions: This symptom is observed when a Cisco 7600 series boots with a large number of VPN interfaces.

  Workaround: There is no workaround.

- CSCsh18070

  Symptoms: Routing protocols may flap on a service instance or routed VPLS (R-VPLS) interface.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured with an Ethernet Services (ES20) line card and any WAN module and/or SIP. The symptom occurs when the traffic through the service instance or R-VPLS interface exceeds the line rate in the egress direction or when the traffic exceeds the shape rate in the class-default class of an MQC policy.

  Workaround: There is no workaround. The symptom is less likely to occur when you reduce the traffic on the port to below the line rate or below the shaping rate.

  Further Problem Description: The symptom occurs because control packets are not treated as high-priority packets on the service instance or R-VPLS interface.

- CSCsh19574

  Symptoms: A Cisco 7600 series takes about 20 minutes to boot completely.

  Conditions: This symptom is observed when the router has a scaled subinterface configuration with 2000 to 4000 subinterfaces. The boot process is adversely affected when the **ip pim** command is configured on the subinterfaces.

  Workaround: There is no workaround.

- CSCsh20354

  1. 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)
     ```

  2. 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.

- CSCsh20479

  Symptoms: IP services that are configured on an active software EoMPLS VC may not process L3 control frames.

  Conditions: This symptom is observed on a Cisco router when an active software EoMPLS VC (that is, when an Xconnect statement is configured via an SVI/VLAN interface) is configured with an L3 IP address and L3 control frames such as L3 ARP or OSPF multicast frames.

  Workaround: Remove the SVI interface and recreate the SVI interface with the L3 IP address before you configure the EoMPLS xconnect statement. Doing so enables IP services first and then the EoMPLS VC, allowing both to function properly.

- CSCsh21398

  Symptoms: A Cisco 7600 series in which a WS-F6700-DFC3BXL module with 256 MB of memory is installed may run out of memory and display memory allocation failure messages such as the following:

  ```
  %SYS-DFC2-2-MALLOCFAIL: Memory allocation of 4188 bytes failed from 0x205336A0,
  alignment 0 Pool: Processor  Free: 56780  Cause: Memory fragmentation

  Alternate Pool: None  Free: 0  Cause: No Alternate pool

   -Process= "XDR LC Background", ipl= 0, pid= 181

   -Traceback= 20412DD8 2041331C 2050227C 2050BD08 205336A8 211642AC 2113B39C 211393B4
  2114C100 2114ADBC 2113721C 21137354 2113794C 21137CE8 211B7C78 21202F10

  %FIB-2-FIBDISABLE: Fatal error, slot 2/0 (2): CEF-Common: no memory

  %ADJ-DFC2-3-ALLOCATEFAIL: Failed to allocate an adjacency

  -Traceback= 20412DD8 2041331C 211A3DE0 211A4414 21129664 21129850 21139294 211393A4
  2114C100 2114ADBC 21e1 3t7o2 1aC  f2a1tal err1or.37354 2113794C 21137CE8 211B7C78
  21202F10

  %COMMON_FIB-DFC2-3-NOMEM: Memory allocation failure for path list in Common CEF
  [0x21139490] (fatal) (0 subsequent failures).

  %COMMON_FIB-DFC2-4-DISABLING: Common CEF is being disabled due to a fatal error.

  %FIB-2-FIBDISABLE: Fatal error, slot 2/0 (2): CEF-Common: no memory

  %XDR-DFC2-6-XDRLCDISABLEREQUEST: Client CEF push requested to be disabled.

  -Traceback= 20412DD8 2041331C 21217E98 211B0C48 211B3760 21155594 21159FF4 21153D4C
  21153F10 204F6448 204F6434

  %COMMON_FIB-DFC2-4-DISABLING: Common CEF is being disabled due to a fatal error.
  ```

  Conditions: This symptom is observed in a scaled configuration (which is typical of broadband deployments) when 28,000 access subinterfaces are created and brought up.

  Workaround: There is no workaround.

- CSCsh22171

  Symptoms: After an MPLS-TE path is rerouted, the Virtual Private LAN Services (VPLS) feature stops decapsulating Spanning Tree Protocol (STP) Bridge Protocol Data Unit (BPDU) frames that are received from a remote PE router. This situation may result in an STP loop.

  Conditions: This symptom is observed on a Cisco 7600 series that functions as a PE router in an MPLS network, that has many MPLS-TE tunnels configured, and that has the **l2protocol-tunnel stp** command enabled.

  Workaround: Enter the **no l2protocol-tunnel stp** command.

- CSCsh22671

  Symptoms: IPsec security associations (SAs) may not be deleted from a spoke.

Conditions: This symptom is observed when the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command is entered on the interface of the hub that is connected to the spoke.

Workaround: Enter the **clear crypto sessions** command on the spoke.

- CSCsh23176

  Symptoms: A router crashes when you unconfigure RIP.

  Conditions: This symptom is observed on a Cisco router and is more likely to occur when there are many RIP routes configured.

  Workaround: Remove all network statements that are defined under the **router rip** command, wait for all RIP routes to age-out, then remove the **router rip** command.

- CSCsh31679

  Symptoms: PVCs that are configured on MFR interfaces may become inactive for some time after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when the active supervisor engine crashes and causes an SSO switchover to occur.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, note that the PVCs do come up after some time. Otherwise, reset the affected line cards.

- CSCsh34529

  Symptoms: An ATM interface configuration may become lost on the standby RP.

  Conditions: This symptom is observed on a Cisco 7600 series when you perform the following steps:

  1. You configure an ATM main interface on a SPA.
  2. You configure PVCs on the ATM main interface.
  3. You shut down the SPA.
  4. You reload the standby supervisor engine and wait until it comes up.
  5. You bring up the SPA from the active RP.

  At this point, the ATM interface configuration is lost on the standby RP.

  This symptom is observed with both 8-port OC-3c/STM-1 ATM SPAs and Circuit Emulation over Packet (CEoP) SPAs.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the standby supervisor engine once more.

- CSCsh34536

  Symptoms: A Circuit Emulation (CEM) group configuration may become lost on the standby RP.

  Conditions: This symptom is observed on a Cisco 7600 series when you perform the following steps:

  1. You configure a CEM interface and groups on a Circuit Emulation over Packet (CEoP) SPA.
  2. You shut down the SPA.
  3. You reload the standby supervisor engine and wait until it comes up.
  4. You bring up the SPA from the active RP.

  At this point, the CEM group configuration is lost on the standby RP.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the standby supervisor engine once more.

- CSCsh35236

  Symptoms: A 20-port Ethernet Services line card (7600-ES20-GE) may crash and a "mac_xid=0x10000" PXF exception may be generated.

  Conditions: This symptom is observed on a Cisco 7600 series under a rare condition when a specific (test) source MAC address triggers the crash and when the router function under stress.

  Workaround: There is no workaround.

- CSCsh35451

  Symptoms: In an HA configuration when the router is in the runversion-switchover state, when you enter the **issu runversion** command, the newly active supervisor engine does not come up fully and causes the standby supervisor engine to crash with "Active_Not_Responding" error messages.

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

  1. You enter the **issu loadversion** command, and you wait for the router to enter the terminal state.
  2. You enter the **issu runversion** command, and you wait for the router to enter the terminal state.
  3. The active supervisor engine crashes, and then moves to the RunVersionSwitchOver (RVSO) state.
  4. The newly active RP and standby RP come up, and you wait for the router to enter the terminal state.
  5. Again, you enter the **issu runversion** command on the active supervisor engine.

  At this point, the symptom occurs.

  Workaround: There is no workaround.

- CSCsh36614

  Symptoms: When Server Load Balancing (SLB) is configured and when policy-based routing is applied to the outbound path, the first response packet (that is, the syn-ack packet) from the real server is process-switched instead of switched via the special switching path.

  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: There is no workaround.

- CSCsh37219

  Symptoms: IPv6 multicast convergence takes 25 to 30 minutes on a Route Switch Processor 720 when an ATM interface on a SIP-200 functions as the uplink between the two routers.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with 32,000 (S,G) entries with 4000 groups from four sources and 16,000 packets per burst with packets that have a size of 64-bytes.

  Workaround: There is no workaround.

- CSCsh39318

  Symptoms: A router may crash when the configured route limit is exceeded. When this situation occurs, the following error message is generated:

  ```
  %MROUTE-4-ROUTELIMIT (x1): [int] routes exceeded multicast route-limit of [dec] - VRF
  [chars]
  ```

Conditions: This symptom is observed on a Cisco 10000 series that is configured for Multicast VPN but is platform-independent.

Workaround: There is no workaround.

- CSCsh40540

  Symptoms: When a service instance is configured for Xconnect, the pseudowire fails to come up, and an "%SW_MGR-SP-3-CM_ERR" error message is displayed.

  Conditions: The symptom is observed on a Cisco 7600 series only when encapsulation is configured as default.

  Workaround: There is no workaround.

- CSCsh40567

  Symptoms: When OAM cells are transported over a local-switched connection that is configured for AAL5 and for which the VPI or VCI do not match at both endpoints, OAM cells are dropped.

  Conditions: This symptom is observed on a Cisco 7600 series on an ATM SPA that is installed in a SIP-200 or on an ATM port adapter that is installed in a FlexWAN or Enhanced FlexWAN module.

  Workaround: Ensure that the VPI or VCI are the same at both endpoints of the local-switched connection.

- CSCsh45829

  Symptoms: An interface that is configured for Xconnect fails to come up.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a Supervisor Engine 32 and that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCsh45862

  Symptoms: When a 24-port channelized T1/E1/J1 ATM CEoP SPA (SPA-24CHT1-CE-ATM) that functions ATM mode is heavily oversubscribed with traffic in one direction (either ingress or egress), the SPA may block all ping packets while still allowing other traffic to pass through. When this situation occurs, interfaces remain up, and there are no other error signals.

  Conditions: This symptom is observed on a Cisco 7600 series and is likely to occur with small packets such as 46-byte packets of an L3 payload.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reload the SPA by entering the **hw-module subslot** *slot*/*subslot* **reload** command.

- CSCsh46540

  Symptoms: A router crashes when the **format disk0:** and **copy tftp: disk0:** commands are executed in parallel.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system when the commands are entered through two different sessions.

  Workaround: Do not enter the above-mentioned commands in parallel.

- CSCsh47823

  Symptoms: CPU usage may become very high. When this situation occurs, a line card may become unable to respond to keepalive polling from the supervisor engine, and the Switch Processor (SP) may reset the line card.

  Conditions: This symptom is observed on a Cisco 7600 series that has a scaled QoS configuration when the Route Processor (RP) sends many configuration changes to the line card.

Workaround: On both the RP and the SP, disable resetting of the line card for keepalive response failures. On the RP, enter the **test scp linecard keepalive disable** command; on the SP, enter the **debug oir no-reset-on-crash** *slot* command.

- CSCsh48705

  Symptoms: VPLS traffic may be dropped from the egress path on a SIP-400.

  Conditions: This symptom is observed on a Cisco 7600 series when the VPLS traffic passes through a traffic engineering tunnel that is protected by FRR. The primary tunnel is on the SIP-400; the backup tunnel is on another line card. The symptom occurs when the following events take place:

  After you have configured FRR and reset the SIP-400, FRR switching occurs and the VPLS traffic is switched to the backup tunnel on the other line card. When the SIP-400 boots, the VPLS traffic is switched back to the primary tunnel as a result of L3 MPLS reconvergence. However, from this time on, the VPLS traffic is dropped from the egress path on the SIP-400.

  Workaround: Remove the FRR configuration, reset the SIP-400, and reconfigure the FRR configuration.

- CSCsh50878

  Symptoms: When a 4-port T3/E3 serial SPA initialization does not complete, a configuration synchronization mismatch may occur and the standby supervisor engine may reload.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured for SSO and occurs after the router has been reloaded multiple times.

  Workaround: While the standby supervisor engine is coming up, enter the **redundancy config-sync ignore mismatched-commands** command on the active supervisor engine.

- 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.

- CSCsh52183

  Symptoms: OSPF VRF processes may consume most of the system memory. Commands such as the **show running-config** command and **show process cpu sorted** do not function.

  Conditions: This symptom is observed on a Cisco 7600 series when OSPF is configured on inside VRFs (IVRFs), front-door VRFs (FVRFs), and Virtual Tunnel Interfaces (VTIs). The more tunnels there are, the earlier the symptom occurs.

  Workaround: Configure only a few OSPF routes in a configuration with IVRFs, FVRFs, and VTIs.

  Alternate workaround: Do not use OSFP, Rather, use EIGRP.

- CSCsh52354

  Symptoms: When you change the **encapsulation dot1q** command from a dual VLAN configuration to a single VLAN configuration by entering the **rewrite ingress tag pop 2 symmetric** command specified for a service instance, the command may be rejected and the standby supervisor engine may reload unexpectedly.

Conditions: This symptom is observed on a Cisco 7600 series when a service instance is configured in the following way:

```
service instance <x> ethernet
encapsulation dot1q <vlan-id> second-dot1q <vlan-id>
rewrite ingress tag pop 2 symmetric
```

Workaround: Disable the **rewrite** command before you change the **encapsulation dot1q** command.

- CSCsh52364

  Symptoms: A 24-port channelized T1/E1 CEoP SPA may not frame its T1 lines properly, causing path code violations to be generated at the remote end.

  Conditions: This symptom is observed on a Cisco 7600 series under rare conditions when the SPA is reloaded. The symptom may not occur with a few pings but could occur when traffic is being processed.

  Workaround: Shut down and bring up the affected port:

  ```
  conf t
  controller (t1|e1) slot/bay/port
  shutdown
  no shutdown
  exit
  ```

- CSCsh53802

  Symptoms: When the PBR Support for Multiple Tracking Options feature is enabled via the **set ip next-hop verify-availability** command and when the first next hop goes down, the router sets the second next hop in software rather than in hardware, even if the second next hop is up and available.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that have at least two next hops.

  Workaround: There is no workaround.

- CSCsh54054

  Symptoms: When a 24-port channelized T1/E1/J1 ATM CEoP SPA (SPA-24CHT1-CE-ATM) that functions ATM mode is heavily oversubscribed with traffic in both the ingress and egress directions, the SPA may generate the following error message and then resets:

  ```
  %SPA_PLIM-3-ERRMSG: SPA-24CHT1-CE-ATM[3/2] (CEMA_INT-3-FATAL_INTERRUPT: Fatal
  Winpath Packet Bus Error interrupt: Bus Error: 8-byte read from 0x401b4000 generated
  by WMM TRS: 1 pc:0x3438 data: r64 address: r58)
  ```

  Conditions: This symptom is observed on a Cisco 7600 series and is likely to occur with packets with sizes of 235 or 265 bytes (that is, L3 payload-size packets).

  Workaround: There is no workaround. However, the symptom corrects itself because the SPA is automatically reset.

- CSCsh54380

  Symptoms: After Fast Reroute (FRR) has rerouted traffic over a backup traffic engineering (TE) tunnel, VCs on an Ethernet Services (ES20) line card may not generate correct statistics.

  Conditions: This symptom is observed on a Cisco 7600 series that has a SIP-600 in which an ES20 line card is installed that is configured for VPLS EoMPLS in a highly scaled configuration with a large number of VPLS VCs that are protected by FRR. The symptom occurs in the following configuration scenarios:

When one interface of the TE tunnel (either the interface for the primary or the backup tunnel) is configured on:

- a port on a SIP-600, or
- a port from 0 through 19 on a 20-port ES20 line card (7600-ES20-GE), or
- the first port (that is, port 0) on a 2-port version ES20 line card (7600-ES20-10G),

and when the other interface of the TE tunnel (either the interface for the primary or the backup tunnel) is configured on:

- a port from 0 through 19 on a 7600-ES20-GE, or
- the second port (that is, port 1) on a 7600-ES20-10G.

Workaround: There is no workaround.

- CSCsh55166

  Symptoms: PIM neighbors on a core interface become lost when traffic is sent.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in a Routed VPLS (R-VPLS) environment when the core interface has PIM enabled but when a switched virtual interface (SVI) that is also configured for R-VPLS does not have PIM enabled.

  Workaround: Configure PIM on the SVI.

- 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.

- CSCsh56902

  Symptoms: The output of the **show mls cef** command shows a hidden VLAN instead of an interface as a VRF tag:

  ```
  1025 === tegigX/X
  ```

  output

  ```
  X.X.X.... VRF1025 x.x.x.x
  ```

  should be...

  ```
  X.X.X... tegigX/X x.x.x.x
  ```

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

  Workaround: Reload the router or shut down and bring up the affected interface. The symptom does not affect proper functionality of the router.

- CSCsh58526

  Symptoms: When the number of Ethernet Virtual Connections (EVCs) exceeds 1000, EVCs flap and the CPU usage in the “Ethernet CFM” process is significantly higher.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when the number of EVCs is in the range of 4000.

  Workaround: Ensure that the number of EVCs is 1000 or smaller.

- CSCsh60202

  Symptoms: Routed VPLS (R-VPLS) multicast packets may flood a SIP-400 on which Ethernet Virtual Circuit (EVC) service instances are configured and may egress the service instances.

  Conditions: This symptom is observed on a Cisco 7600 series when a bridge-domain VLAN matches the R-VPLS switched virtual interface (SVI).

  Workaround: There is no workaround.

- CSCsh61851

  Symptoms: A PIM neighborship does not come up on an MDT tunnel when VRFs are removed and added back immediately on PE routers.

  Conditions: This symptom is observed on Cisco 7600 series routers that run Cisco IOS Release 12.2(33)SRB.

  Workaround: Wait for 3 to 4 minutes after you have removed the VRFs on the PE routers so that the backbone entries that are associated with the VRFs expire. Then, add back the VRFs.

  Further Problem Description: The VPN ID is not re-used when a VRF is removed and recreated. This situation results in stale VPN information on the supervisor engine and DFC because backbone entries that are associated with the old VRF can exist until they expire. When a new VPN ID is issued because you recreate the VRF, the hardware entry may not be programmed correctly because of the stale VPN information, preventing the PIM neighborship from being established over the MDT tunnel.

- CSCsh61926

  Symptoms: The following error message may be generated appears on a Cisco router that is configured for MPLS:

  ```
  LSD_HA-3-GENERAL: Cannot chkpt now
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a large number of VRFs.

  Workaround: There is no workaround.

- CSCsh62612

  Symptoms: A standby supervisor engine may reload continuously while attempting to boot after a supervisor engine switchover has occurred. In this situation, the active supervisor engine functions fine.

  Conditions: This symptom is observed during the bulk synchronization of a configuration from the active supervisor engine to the new standby supervisor engine while the standby supervisor engine comes up after a supervisor engine switchover has occurred.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, reload both the active and standby supervisor engines.

- CSCsh64335

  Symptoms: A router may crash when you enter the **mkdir** command to create a directory with a length of more than 127 characters and when you query this directory via SNMP.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system.

  Workaround: There is no workaround.

- CSCsh65083

  Symptoms: A Circuit Emulation over Packet (CEoP) SPA may reload when an SSO switchover or APS switchover occurs. Note that the SPA functions normally after it has reloaded.

Conditions: This symptom is observed on a Cisco 7600 series when the following conditions are met:

- Both Circuit Emulation (CEM) and ATM are configured on the SPA.
- ATM traffic is being processed on the SPA.
- Multiple SSO or APS switchovers occur.

Workaround: Avoid multiple SSO or APS switchovers.

- 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.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur with a FlexWAN.

- CSCsh67160

  Symptoms: CEF consistency checkers may become disabled, and the following message may be generated:

  ```
  %CEF consistency checkers currently offline (Switchover in progress)
  ```

  Conditions: This symptom is observed on a Cisco router that has the **ip cef** command enabled when an SSO switchover occurs. The symptom does not occur when the **ipv6 cef** command is enabled.

  Workaround: Do not enter the **ip cef** command. Rather, enter the **ipv6 cef** command.

- CSCsh69341

  Symptoms: In a Server Load Balancing (SLB) configuration, input features (except for Policy Based Routing [PBR]) that should not be processed are unexpectedly executed in a special switching path.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch that runs Cisco IOS Release 12.2SXH and Cisco 7600 series that runs Release 12.2SXH or Release 12.2(33)SRB and that are configured with a Supervisor Engine 720.

  Workaround: There is no workaround.

  Further Problem Description: The symptom may cause SLB to behave in an unexpected way. For example, when an input access control list (ACL) is applied on an interface, SLB is supposed to bypass the ACL, which is considered an input feature, so SLB packets can reach their destination without a problem. However, because of the symptom, the ACL is active and may stop SLB packets from reaching their destination.

- CSCsh72267

  Symptoms: A PVC that is configured on an ATM interface that is configured for cell packing may not receive the MNCP and MCPT parameters from the ATM interface. (MNCP = Maximum cells packed in one MPLS packet; MCPT = Maximum time to wait to pack the cells in one MPLS packet.)

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

  Workaround: Do not configure cell packing on the ATM interface. Rather, configure cell packing directly on the PVC.

- CSCsh72329

  Symptoms: When APS is triggered by a soft OIR of a working 1-port channelized OC-3 STM1 ATM CEoP SPA (SPA-1CHOC3-CE-ATM), some of the CEM VCs may take more than 150 seconds to come up. Because of this situation, there may be a delay in traffic recovery following the APS switchover.

  Conditions: This symptom is observed on a Cisco 7600 series when you perform a soft OIR on the SPA-1CHOC3-CE-ATM by entering the **hw-module subslot** *slot/subslot* **reload** command.

  Workaround: There is no workaround. However, the router recovers automatically.

- CSCsh72407

  Symptoms: When cell packing is configured on a PVP between two PE routers, the MNCP parameter is not exchanged over an AToM L2TPv3 connection. The PE router shows that the MNCP of the peer is 1, but this should be a greater value. (MNCP = Maximum cells packed in one MPLS packet.)

  Note that a ping from one PE router to the other works fine, the Layer 2 tunnel is up, and the connection between CE routers work fine.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured for Xconnect. The symptom is platform-independent.

  Workaround: Do not use an L2TPv3 connection. Rather, use an MPLS connection. If this is not an option, there is no workaround.

- CSCsh73675

  Symptoms: An Ethernet Virtual Connection (EVC) that is configured for EoMPLS or another feature may not pass traffic after the router has been reloaded.

  Conditions: This symptom is observed on a Cisco 7600 series with a scalable EVC configuration of 16,000 EVCs on the same Ethernet Services (ES20) line card. The symptom occurs very rarely and is related to a peculiar timing issue.

  Workaround: There is no workaround.

- CSCsh73935

  Symptoms: A router may reload when you perform an snmpwalk on the ciscoMvpnMrouteMdtTable.

  Conditions: This symptom is observed when all of the following conditions are present:

  – IP multicast routing is enabled on a VPN routing/forwarding instance (VRF)
  – This VRF is associated with an interface.
  – The Multicast Distribution Tree (MDT) default group address is not configured for the VRF.

  Workaround: Configure the MDT default group address for the VRF by entering the **mdt default** *mdt group* command in VRF configuration mode.

- CSCsh74127

  Symptoms: ISIS adjacencies may not be established.

  Conditions: This symptom is observed on a Cisco 7600 series where the ISIS adjacency is configured to be established over an Ethernet Services (7600 ES20) line card with QinQ subinterfaces that are configured to support double-tagged packets when the default MTU size is 1500 bytes.

  Workaround: Configure the MTU to be 1504 bytes.

- CSCsh75001

  Symptoms: After a SIP-400 or the router reloads, interfaces remain down until you enter the **shutdown** command followed by the **no shutdown** command on the affected interfaces.

  Conditions: This symptom is observed on a Cisco 7600 series that has a SIP-400 in which the following SPAs are installed:

  - a 2-port GE SPA (SPA-2X1GE)
  - a 1-port channelized OC-3 STM1 ATM CEoP SPA (SPA-1CHOC3-CE-ATM)

  The interfaces of these SPA are configured with more than 3000 Ethernet Virtual Connection (EVC) flexible instances that are configured for QoS.

  Workaround: There is no workaround.

  Further Problem Description: Configuring more than 3000 EVC instances with QoS on a SIP-400 in which both a SPA-2X1GE and a SPA-1CHOC3-CE-ATM are installed is not supported. A large configuration of EVC instances with QoS can be achieved only without a SPA-1CHOC3-CE-ATM in the SIP-400 in which the SPA-2X1GE is installed.

- CSCsh75176

  Symptoms: A standby RP with a VRF configuration may reload continuously.

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

  Workaround: There is no workaround.

- CSCsh75457

  Symptoms: The RP may crash during the boot process of the router.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that is configured with QoS service policies.

  Workaround: There is no workaround.

- CSCsh78154

  Symptoms: When an interface on a SIP-400 has many subinterfaces with QoS input policies configured, some packets may drop in the form of input errors. The drop rate is very low, typically less than 0.001 percent.

  Conditions: This symptom is observed on a Cisco 7600 series and occurs on Gigabit Ethernet (GE) and POS interfaces (but not on ATM interfaces) when the following conditions are met:

  - The interface has a few hundred subinterfaces per port, each configured with a QoS input policy.
  - Small- to medium-sized packets up to 500 bytes are processed.
  - A moderate to heavy traffic volume is processed. The volume depends on the packet size, for example: 64-byte packets at about 20 percent of the GE line rate, 128-bype packets at about 50 percent of the GE line rate, 256-byte packets at about 85 percent of the GE line rate, and so on.

  Workaround: There is no workaround. The packet drop rate is unnoticeably low, but detectable in performance tests.

- CSCsh80337

  Symptoms: An exception may occur on the active and standby Supervisor Engine 720 modules, they enter ROMmon, and all configurations may become lost.

Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when the following conditions occur:

1. There is one Supervisor Engine 720 in the chassis.
2. You insert another Supervisor Engine 720 that contains another Cisco IOS software image into the chassis. The compact flash on this supervisor engine is replaced with another one that also contains Cisco IOS Release 12.2(33)SRB.
3. You attempt to boot the newly inserted Supervisor Engine 720 as the standby supervisor engine with Release 12.2(33)SRB, it encounters an exception, and enters ROMmon.
4. The active Supervisor Engine 720 also encounters en exception and enters ROMmon.
5. You boot the active Supervisor Engine 720 manually.

At this point, all configurations become lost.

Workaround: There is no workaround.

- CSCsh83467

  Symptoms: A standby Supervisor Engine 720 may reset when an entire Circuit Emulation (CEM) configuration is removed and then reconfigured.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when the **recovered-clock** command is present in the removed configuration.

  Workaround: Do not remove an entire CEM configuration.

  Alternate Workaround: Disable the **recovered-clock** command before you remove and then reconfigure an entire CEM configuration.

- CSCsh84531

  Symptoms: After an SSO switchover has occurred, a large number of Circuit Emulation (CEM) circuits may remain down.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a SIP-400 in which a Circuit Emulation over Packet (CEoP) SPA is installed when the router has a very high CPU usage during the SSO switchover.

  Workaround: There is no workaround to prevent the symptom from occurring. Perform a software or hardware OIR of the SIP-400 to recover the CEM circuits.

- CSCsh90556

  Symptoms: Traffic may fail to match the VLAN TCAM, causing traffic to be dropped from a SPA that is installed in a SIP-400.

  Conditions: This symptom is observed on a Cisco 7600 series when an Xconnect service is configured and when double-tagged frames are sent via a service instance that is configured with single-tag encapsulation.

  Workaround: Configure two service instances, as in the following examples:

  – A service instance to handle single-tagged packets with VLAN ID = 100:

    ```
    service instance 10 ethernet
    encapsulation dot1q 100
    ```

  – A service instance to handle double-tagged packets with the outer tag = 100:

    ```
    service instance 20 ethernet
    encapsulation dot1q 100 second-dot1q any
    ```

- CSCsh90762

  Symptoms: The hardware adjacencies that correspond to 6PE aggregate labels may be wrongly programmed.

  Conditions: This symptom is observed on a Cisco 7600 series that functions as a 6PE router.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interfaces that are associated with the IPv6 prefixes that correspond to the affected 6PE aggregate labels.

- CSCuk60927

  Symptoms: A variety of symptoms may occur on a Cisco router such as a Cisco 7600 series that is configured for distributed CEF (dCEF) switching because of loss of interprocess communication (IPC) messages between line cards and the RP. These symptoms may include the following:

  – Disabling of dCEF switching on the line card after the router has booted or after an SSO switchover, microcode reload, or OIR.
  – Loss of statistics from the line cards.

  Conditions: This symptom is observed only when either there are high quantities of statistics being reported (for example, for very large numbers of AToM endpoints) or when the router synchronizes a very large configuration to the standby RP during the boot process.

  Workaround: In most conditions, entering the **clear cef linecard** command re-enables the line cards.

  Further Problem Description: IPC messages are used for a variety of purposes: most commonly for statistics reporting, but also when a line card is brought up and when dCEF is enabled. The loss of these IPC messages gives rise to one of the symptoms. The probability of drops occurring is normally negligible except in situations in which there is a very high volume of IPC traffic. This high traffic volume may occur when the router synchronizes large configurations to the standby RP and also when extremely large numbers of statistics are sent via IPC.

  Note Note: NetFlow statistics are not sent via IPC and are therefore not affected by nor do they trigger the symptoms.

- 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.

TCP/IP Host-Mode Services

- CSCee32814

  Symptoms: Port numbers for TCP connections originating from the router are chosen in an incremental way making it easy to predict them.

  Conditions: Any TCP connection on the router using non-well-known port numbers is subject to this behavior.

  Workaround: There is no workaround.

- CSCsh36234

  Symptoms: File paths that start with a double slash may fail to open the file successfully.

  Conditions: This symptom is observed when you enter the **install** command with the **scp** keyword, that is when an SCP application functions as the source.

  Workaround: Move the file to another location where the double slash is not required.

  Alternate Workaround: Use another protocol such as RCP or TFTP to transfer the file.

Wide-Area Networking

- CSCek64788

  Symptoms: A router crashes because of memory corruption. The crashinfo points to the VPDN call manager.

  Conditions: This symptom is observed on a Cisco router when L2TP Active Discovery Relay for PPPoE is enabled.

  Workaround: There is no workaround.

- CSCsg90645

  Symptoms: In an L2TP Dial-Out configuration with a RADIUS or TACACS server for AAA services, the remote name is wrongly mapped to the secondary IP address of the LNS instead of to the primary IP address.

  Conditions: This symptom is observed on a Cisco router that is configured for VPDN. Note that local authentication and authorization function fine.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRB

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(33)SRB. This section describes only severity 1, severity 2, and select severity 3 caveats.

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.

- CSCei37916

  Symptoms: A Cisco GGSN does not function properly when wait-accounting and AAA Broadcast Accounting are configured on an APN. When the first RADIUS server responds to an Accounting Start message, the GGSN establishes the PDP context without waiting for responses from all other RADIUS servers. Under a stress condition, the GGSN may reload.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4 and GGSN Release 5.2 and occurs only when both wait-accounting and AAA Broadcast Accounting are configured together on an APN. Note that the symptom is not release-specific.

  Workaround: There is no workaround.

- CSCej42445

  Symptoms: MS-CHAP authentication or MS-CHAP and PAP authentication may fail.

  Conditions: This symptom is observed on a Cisco router that is configured to use TACACS+ and MS-CHAP for authentication.

  Workaround: There is no workaround.

- CSCek33076

  Symptoms: A RADIUS progress code is incorrectly reported for a call that fails at IPCP. The progress code reports that the Link Control Protocol (LCP) is the open state.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.4(3a) and that is configured for AAA. The symptom is not release-specific.

  Workaround: There is no workaround.

- CSCek37174

  Symptoms: When you configure RADIUS servers via the AAA-SERVER-MIB, the expected behavior is that the last defined RADIUS server receives the lowest priority, but this does not occur.

  Conditions: This symptom is observed on a Cisco router that is configured for AAA and that runs Cisco IOS Release 12.4 or Release 12.4T. However, the symptom is release-independent.

  Workaround: There is no workaround.

- CSCek52249

  Symptoms: A Cisco router crashes when the **default dest-ip** command is entered in IPSLA jitter, UDP Echo and TCP Connect operations.

  Conditions: The issue is seen when the **default dest-ip** command is entered.

  Workaround: There is no workaround.

- CSCek58338

  Symptoms: A Cisco 7600 series may crash because of memory corruption in the chunk memory.

  Conditions: This symptom is observed when both the Embedded Resource Manager (ERM) and Bidirectional Forwarding Detection (BFD) are configured.

  Workaround: Disable BFD.

- CSCin60071

  Symptoms: After tunnel sessions have flapped on an L2TP Access Concentrator (LAC) or an L2TP Network Server (LNS), the sessions may be re-established on the wrong tunnels.

  Conditions: This symptom is observed when there is a high call rate and a high call volume.

Workaround: Enable the **radius-server source-ports extended** global configuration command.

- CSCin99433

  Symptoms: Without configuring any command related to Kerberos other than a Kerberos password command, a configuration synchronization failure may occur because of a PRC mismatch.

  Conditions: This symptom is observed when you boot a Cisco router that is configured for AAA.

  Workaround: There is no workaround.

- CSCsa43465

  Symptoms: Users may be able to access root view mode (privilege level) 15 without entering a password.

  Conditions: This symptom is observed on a Cisco router that has the Role-Based CLI Access feature enabled and occurs when the **none** keyword is enabled in the default login method list.

  For example, the symptom may occur when you enter the **aaa authentication login default group tacacs+ none**. When the TACACS+ server is down, users are allowed to enter non-privileged mode. However, users can also access the root view through the **enable view** command without having to enter a password.

  Workaround: Ensure that the **none** keyword is not part of the default login method list.

  Further Problem Description: The fix for this caveat places the authentication of the **enable view** command in the default login method list.

- CSCsb08386

  Symptoms: A router crashes when you enter the **show ip bgp regexp** command.

  Conditions: This symptom is observed on a Cisco router when BGP is being updated.

  Workaround: Enable the new deterministic regular expression engine by entering the **bgp regexp deterministic** command and then enter the **show ip regexp** command. Note that enabling the new deterministic regular expression engine may impact the performance speed of the router.

- CSCsb30875

  Symptoms: When the **aaa accounting system** command is enabled, the active RP may hang after an RPR+ switchover has occurred.

  Conditions: The symptom is observed on a Cisco gateway or router when the console session is closed and reopened for the newly active RP after the RPR+ switchover has occurred.

  Workaround: Do not close and reopen the console session for the newly active RP.

  Alternate Workaround: Disable the **aaa accounting system** command.

- 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.

- CSCsd10306

  Symptoms: IP SLA packets may be dropped in a network. These dropped packets may also cause a buffer leak on some Cisco routers. The frequency of the symptom is very low; less then 1 percent of the IP SLA packets are dropped.

  Conditions: This symptom is observed for IP SLA packets to which an MPLS label is applied on the source router.

Workaround: There is no workaround.

Further Problem Description: The IP SLA packets that are dropped have a corrupted IP header.

- CSCsd26248

  Symptoms: A memory leak may occur in the RADIUS process on a router that is configured for dot1x authentication but that does not have the **aaa authentication dot1x** command enabled. The memory leak may consume all free memory.

  Conditions: This symptom is observed when the router receives attribute 24 (state) or attribute 25 (class) from a RADIUS server.

  Workaround: There is no workaround.

- CSCsd37284

  Symptoms: A router may crash when you use Remote Network Monitoring (RMON) to copy a configuration to the running configuration.

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCeg74543. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeg74543. 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.

- 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.

- CSCse10074

  Symptoms: The active RP may crash when traps are sent to a host to which an SNMPv3 user is assigned.

  Conditions: This symptom is observed only when an SNMPv3 user is configured with security level noAuthNoPriv or authPriv, when the same SNMPv3 user is assigned to the host through the **snmp-server host** command, and when this command includes the **priv** keyword. This is an improper configuration.

  For example, the symptom occurs when traps are triggered after the following software configurations has been applied:

  ```
  snmp-server user TESTUSER TESTUSER v3
  snmp-server group TESTUSER v3 priv notify *tv.FFFFFFFF.FFFFFFFF.FFFFFFFF.F
  snmp-server host 10.1.1.10 version 3 priv TESTUSER
  snmp-server enable traps
  ```

  Workaround: Do not create an improper configuration.

- CSCse38956

  Symptoms: A router crashes when you change the authentication method after the user on the client side has entered the user name and is prompted to enter the password but has not yet entered the password.

Conditions: This symptom is observed when you disable the **aaa authentication enable default group radius** command and enable the **aaa authentication enable default group tacacs** command, or the other way around, before the user on the client side has entered the password.

Workaround: There is no workaround.

- CSCse49728

  Symptoms: SNMPv3 informs are not sent out after a device reload.

  Conditions: This symptom is observed when SNMPv3 informs have been configured, and the device is reloaded.

  Workaround: Re-enter any of the **snmp-server host** commands.

- CSCse66080

  Symptoms: A memory leak may occur in the Entity MIB API process.

  Conditions: This symptom is observed when an entity is registered with the same name as an entity that is already registered.

  Workaround: There is no workaround.

- CSCsf19881

  Symptoms: A Cisco 7600 series crashes when you remove AAA commands.

  Conditions: This symptom is observed when you remove the **aaa accounting system default** command.

  Workaround: Do not remove the **aaa accounting system default** command. If this is not an option, there is no workaround.

- CSCsg43322

  Symptoms: When you attempt to configure an authentication, authorization, and accounting (AAA) list for a network, the following error message may be generated:

  ```
  AAA: No free accounting lists for "network".
  ```

  Conditions: This symptom is observed on a Cisco router that has not yet reached its maximum of 1024 authentication lists, 1024 authorization lists, and 1024 accounting lists.

  Workaround: There is no workaround.

- 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.

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** 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.

- 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.

Interfaces and Bridging

- CSCed79345

  Symptoms: A router crashes when you enter the **default/no bridge-group** *bridge group* **subscriber-loop-control** interface configuration command.

  Conditions: This symptom is observed when there are no existing bridge-group configurations on the router.

  Workaround: There is no workaround.

- 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.

- CSCek46996

  Symptoms: An Enhanced FlexWAN Fast Ethernet port adapter cannot support a VPN in crypto connect mode unless the port can immediately transition to promiscuous mode when you enter the **crypto connect** command on the VLAN interface.

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

Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCse61893

  Symptoms: A ping from a channelized T3 (CT3) port adapter may fail.

  Conditions: This symptom is observed on a Cisco platform that is configured with a CT3 port adapter that functions in unchannelized mode.

  Workaround: There is no workaround.

- CSCuk61108

  Symptoms: Packets may become corrupted with a faulty VLAN tag when they are forwarded over an FE interface.

  Conditions: This symptom is observed when the FE interface has subinterfaces that are configured for dot1q encapsulation.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCef70161

  Symptoms: External BGP neighbors that are configured in the IPv4 VRF address-family context may fall into different update groups, even if the outbound policy is identical. This situation slightly reduces the overall scalability because BGP cannot use update replication when sending updates to the neighbors.

  Conditions: This symptom is observed on a Cisco router and is both release- and platform-independent.

Workaround: There is no workaround.

Further Problem Description: The symptom does not affect neighbors that are configured in the global IPv4 address-family context.

- CSCeg57155

  Symptoms: A ping, Telnet traffic, FTP traffic, and trace route traffic across a VRF-aware NAT do not function.

  Conditions: This symptom is observed on a Cisco router that is configured for VRF-aware NAT only when the router is not directly connected to a gateway.

  Workaround: There is no workaround.

- 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.

- CSCek24597

  Symptoms: The BGP Support for Next-Hop Address Tracking feature fails.

  Conditions: This symptom is observed when the BGP Event Process is terminated after BGP has been up.

  Workaround: There is no workaround.

- CSCek31478

  Symptoms: When the access control list (ACL) associated with a multicast boundary is modified to permit a statically joined group that has previously been denied by the boundary, the change does not take effect and the group continues to be blocked.

  This issue also affects the static group memberships underlying MVPN tunnels, disrupting connectivity across them.

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(28)S4 or Release 12.0(32)S but appears to be platform- and release-independent.

  Workaround: Disable and re-enter the **ip multicast boundary** command.

  Alternate Workaround: Enter the **clear ip mroute *** command.

- CSCek32244

  Symptoms: Not all classful networks are locally generated in the BGP table.

  Conditions: This symptom is observed on a Cisco router that has the **auto-summary** command enabled and occurs when classful networks are provided before the routes are made available in the routing table.

  Workaround: There is no workaround.

- CSCek36037

  Symptoms: After a switchover has occurred or when the router is booted, BGP sessions flap.

Conditions: This symptom is observed on a Cisco router that is configured with 1200 BGP peers, a keepalive value of10 seconds, and a holdtime value of 30 seconds.

Workaround: There is no workaround.

- CSCek36056

  Symptoms: When you enter the **ipv6 pim bsr candidate bsr ipv6-address** command, the IPv6 address does not show in the output of the **show running-config** command.

  Conditions: This symptom is observed when you attempt to configure a Cisco router to be an IPv6 candidate bootstrap router (BSR). The symptom does not occur when you configure the router to be an IPv4 BSR.

  Workaround: There is no workaround.

- 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).

- CSCek42700

  Symptoms: A network and host-based configuration download over serial HDLC with an IP address obtained via SLARP fails.

  Conditions: This symptom has been observed with a router that has no startup- configuration (after using the **write erase** command) but is staged for autoinstall over a serial link. An IP address is obtained, but the download fails with the following error message:

  ```
  %Error opening tftp://255.255.255.255/network-confg (Socket error)
  %Error opening tftp://255.255.255.255/cisconet.cfg (Socket error)
  ```

  Without this feature, router deployment with automatic configuration download at remote sites over a serial interface is not possible.

  Workaround: Use another method of autoinstall if possible, or pre-configure the router before deployment.

- 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. However, the symptom is not platform-dependent.

  Workaround: There is no workaround.

- CSCek58880

  Symptoms: A Cisco router that has an interface that is configured for MPLS TE and OSPF may crash when you first remove the OSPF process and then modify the OSPF cost on the interface.

Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software images that integrates the fix for caveat CSCse41174 when the following sequence of events occurs:

- You enter the **ip ospf cost** command on an interface in the MPLS TE area.
- You enter the **no router ospf** *process-id* command on the interface in the MPLS TE area.
- You change the OSPF cost on the interface in the MPLS TE area.

A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse41174. 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.

- CSCek68270

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

  Conditions: This symptom is observed on a Cisco router that contains an 0.0.0.0/0 address in the EIGRP topology with multiple next hops that change in quick succession.

  Workaround: Limit the 0.0.0.0/0 address to a single next hop.

- 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.

- CSCsb50606

  Symptoms: Memory usage in the "Dead" process grows gradually until the memory is exhausted. The output of the **show memory dead** command shows that many "TCP CBs" are re-allocated. Analysis shows that these are TCP descriptors for non-existing active BGP connections.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(13), that has an NPE-G1, and that functions as a PE router with many BGP neighbors. However, the symptom is not platform-specific, nor release-specific.

  Workaround: Reload the router. I this is not an option, there is no workaround.

- CSCsb69773

  Symptoms: A router may crash during the redistribution of OSPF, EIGRP, RIP, and static routes.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and NSF after a switchover from the primary RP to the secondary RP has occurred.

  Workaround: There is no workaround.

- CSCsc00378

  Symptoms: Changes in an export map are not picked up by the BGP Scanner.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when you apply an export map to a VRF and when the interface that connects the PE router to a CE router is configured for OSPF.

  Workaround: Enter the **clear ip ospf process** command to enable the BGP Scanner to pick up the changes in the export map.

- CSCsc33408

  Symptoms: A router reloads unexpectedly when you unconfigure a static route.

  Conditions: This symptom is observed when you first configure the static route for a BGP and IPv4 multicast address family, then clear the BGP routes, and then unconfigure the static route.

  Workaround: There is no workaround.

- CSCsc36517

  Symptoms: A router reloads unexpectedly when a continue statement is used in an outbound route map.

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

  Workaround: There is no workaround.

- CSCsc41694

  Symptoms: A router may hang when you enter the **no router bgp** command.

  Conditions: This symptom is observed on a Cisco AS5400 and Cisco AS5850 but may also occur on other platforms.

  Workaround: There is no workaround.

- CSCsc46337

  Symptoms: When about thousand eBGP connections are opened between two routers that are connected back-to-back, additional point-to-point eBGP connections between the routers are not established even if IP connectivity between the BGP next-hops is provided.

  Conditions: This symptom is observed when one Cisco router functions as a PE router and the other Cisco router functions as a CE router that has VRF-lite configured.

  Workaround: Reload the PE router to enable all sessions to become established, including the ones that previously were not established.

- CSCsc67367

  Symptoms: The **set ip next-hop in-vrf** *vrf-name* command does not work in conjunction with import maps.

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

  Workaround: There is no workaround.

- CSCsc73436

  Symptoms: High CPU usage may occur and the table versions of BGP peers are reset to zero.

  Conditions: This symptom is observed when you update a complex policy on a Cisco router that has a complex configuration of BGP peers.

  Workaround: There is no workaround.

- CSCsc75426

  Symptoms: A router that is configured for BGP and that has the **ip policy-list** command enabled may unexpectedly reload because of a bus error or SegV exception.

  Conditions: This symptom is observed when BGP attempts to send an update with a “bad” attribute.

  Workaround: There is no workaround.

- CSCsc78813

  Symptoms: While using NAT in an overlapping network configuration, the IP address inside a DNS reply payload from the nameserver is not translated at the NAT router.

Conditions: This symptom is observed on a Cisco router that has the **ip nat outside source** command enabled.

Workaround: There is no workaround.

- CSCsd03021

  Symptoms: When loading a large link state database from a third-party vendor router that runs Cisco IOS software, the CPU usage by OSPF may become very high, the router may generate CPUHOG messages, and it may take a long time to reach the FULL state, or the FULL state is not reached.

  Conditions: These symptoms are observed in an environment in which packet drops occur. When the link state request that is sent from the Cisco IOS router is dropped, the routers may still continue to exchange DBD packets. However, the link stay request list on the Cisco IOS router may become long, and it may take a lot of CPU usage to maintain it.

  Workaround: There is no workaround.

  Further Problem Description: See also caveat CSCsd38572.

- 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.

- CSCsd32373

  Symptoms: Multipath load-balancing may not function for internal BGP (iBGP) paths, and routes are not learned through multipath routing, even after you have cleared BGP.

  Conditions: This symptom is observed after an RP switchover has occurred.

  Workaround: There is no workaround.

- CSCsd41237

  Symptoms: Import maps that are applied to VRFs do not take effect. Routes that are received with imported route targets are not filtered by the import route map.

  Conditions: These symptoms are observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that run Cisco IOS Release 12.2(18)SXF. However, the symptoms are both platform- and release-independent.

  Workaround: There is no workaround.

- CSCsd52667

  Symptoms: When you alter the configuration of the **ip nat pool** command, the router may hang, crash, or both.

Conditions: This symptom is observed on a Cisco router when you enter the following commands in sequence:

ip nat pool address 255.255.255.255 255.255.255.255

ip nat pool no address 255.255.255.255 255.255.255.255

or

no ip nat pool *name*

Workaround: There is no workaround.

- CSCsd67768

  Symptoms: Sessions may flap often on a router that has 1200 BGP peers and that is configured with a keepalive value of 10 seconds and a holdtime value of 30 seconds.

  Conditions: This symptom is observed on a Cisco router that has about 1600 interfaces and a large numbers of QoS policies.

  Workaround: Keep the keepalive and holdtime values at the default settings of respectively 60 seconds and 180 seconds. Reduce the load on router by reducing the number of interfaces and QoS policies.

- 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.

- CSCsd77247

  Symptoms: PPPoEoQinQ sessions fail to reconnect.

  Conditions: This symptom is observed on a Cisco router that has 31,000 sessions when there is one session per subinterface. The symptom occurs when you shut down the main interface, bring it up again, and then attempt to reconnect the PPPoEoQinQ sessions.

  Workaround: There is no workaround.

- CSCsd84489

  Symptoms: A platform that is configured for Open Shortest Path First (OSPF) and incremental Shortest Path First (SPF) may crash when changes occur in the OSPF topology.

  Conditions: This symptom is observed on a Cisco platform that has the **ispf** command enabled when changes occur in the OSPF topology that cause the intra-area routes to be updated.

  Workaround: Disable the **ispf** command.

- CSCsd89569

  Symptoms: The output of the **show ip interface brief** command shows inconsistent output with the following extra message at the beginning:

  ```
  Any interface listed with OK? value "NO" does not have a valid configuration
  ```

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

  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.

- 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.

- CSCse07118

  Symptoms: A router may reload unexpectedly when you enter the **transmit-interface** interface configuration command on an interface that has a point-to-point OSPF adjacency.

  Conditions: This symptom is observed on a Cisco router when the OSPF network type is configured as point-to-point, either because the interface is, for example, a serial interface, or because the **ip ospf network point-to-point** interface configuration command is enabled on the interface.

  Workaround: When there is an OSPF adjacency on the interface that is being configured, first enter the **shutdown** interface configuration command before you enter the **transmit-interface** interface configuration command.

- CSCse19737

  Symptoms: The **auto-summary** command does not function.

  Conditions: This symptom is observed on a Cisco router that is configured for IPv4 multicast or IPv4 unicast.

  Workaround: There is no workaround.

- CSCse41174

  Symptoms: An Area Border Router (ABR) may reload when you unconfigure OSPF.

  Conditions: This symptom is observed on a Cisco router that functions as an ABR and that has a TE tunnel when OSPF advertises the outgoing TE tunnel interface in one area and the TE tunnel as a forwarding adjacency in another area.

  Workaround: There is no workaround.

- 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.

- CSCse44079

  Symptoms: The CPU usage may reach 100 percent in the IGMP Input process when a ULD interface is down.

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.

- CSCse51804

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

  1. Symptom 1: A DMVPN tunnel may flap at regular intervals. The NHRP cache entry at the hub expires a long time before its expiration time.

     Condition 1: These symptoms are observed on a Cisco router that runs Cisco IOS Release 12.4 when the DMVPN tunnel is up and when you enter the **show ip nhrp brief** and **clear ip nhrp** commands. When the tunnel comes up again (because of the NHRP registration by the spoke), the NHRP cache entry expires a long time before its expiration time.

     Workaround 1: Do not enter the **show ip nhrp brief** command.

  2. Symptom 2: A DMVPN tunnel may flap at regular intervals. The NHRP cache entry at the hub expires a long time before its expiration time.

     Condition 2: These symptoms are observed on a Cisco router that runs Cisco IOS Release 12.4(6)T or a later release and occurs without any specific action.

     Workaround 2: There is no workaround.

  Further Problem Description: These symptoms are not release-specific.

- CSCse66732

  Symptoms: If Spatial Reuse Protocol (SRP) is used, Enhanced Interior Gateway Routing Protocol (EIGRP) does not respond to the ring drop notification from the interface.

  Conditions: This symptom is observed if SRP is used with EIGRP.

  Workaround: There is no workaround.

- CSCse68877

  Symptoms: A label mismatch may occur between the CEF table and the BGP table, and a new label may not be installed into the CEF table.

  Conditions: This symptom is observed after a BGP flap has occurred on a Cisco router that is configured or MPLS VPN but that does not function in an inter-autonomous system and that does not have multiple VRFs.

  Workaround: There is no workaround. After the symptom has occurred, enter the **clear ip route** command for the affected VRF.

- 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.

- CSCsf02935

  Symptoms: A router that is configured for OSPF Sham-Link and BGP redistribution may crash.

  Conditions: This symptom is observed only in network topologies with OSPF routes that traverse two or more sham links. For example, the symptom may occur in a hub-and-spoke topology with sham links between the hub and two or more individual spokes. This symptom was observed on a Cisco 10000 series but may also occur on other platforms.

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.

- 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 "Standby-Hot" state.

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

- CSCsg32482

  Symptoms: The standby RP does not recover after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco router that functions in an MPLS Traffic Engineering - DiffServ Aware (DS-TE) configuration and that has multiple subinterfaces that have the **ip rsvp bandwidth** command enabled.

  Workaround: 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.

- CSCsg52336

  Symptoms: A router may crash when you remove an unused and unassigned VRF by entering the **no ip vrf** *vpn-name* command.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that has the Multi-VRF capability for OSPF routing configured along with other VRFs that are unused and unassigned.

  Workaround: There is no workaround.

- 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.

- CSCsg59699

  Symptoms: The OSPFv3 cost on PortChannel interfaces that is calculated based on the interface bandwidth may not be correct.

  Conditions: This symptom is observed on a Cisco router when OSPF functions in IPv6 router configuration mode and when the **auto-cost reference-bandwidth** command is enabled.

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

- CSCsg66635

  Symptoms: The IGP metric may be missing from the TE database.

  Conditions: This symptom is observed on a Cisco router when TE is configured on a subinterface and when you enter the **no shutdown** interface configuration command on the physical main interface.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the subinterface on which TE is configured.

- CSCsg71344

  Symptoms: On a router that is configured for SSM and that is connected to an upstream router via two interfaces, when one of the interfaces is shut down and brought up again, a PIM Join message is not sent.

  Conditions: This symptom is observed on a Cisco router that is connected to an upstream router via an RPF interface. When the interface of the upstream router that connects to the RPF interface is shut down, the PIM Join message is sent via the other interface on the Cisco router. However, when the interface of the upstream router that connects to the RPF interface is brought up again, the PIM Join message is not sent again, preventing IPv6 multicast from functioning properly.

  Workaround: There is no workaround.

- CSCsg83966

  Symptoms: Paths that are imported via VPN may be missing from the VRF. For example, paths that are imported from the same route distinguisher (RD) may be missing from the VRF.

  The route map that is specified in the **import ipv4 unicast map** *route-map* command is meant to be applied to paths that are imported into the VRF from the global table. However, the route map is also incorrectly applied to VPN paths during the VPN import process. When the route map filters some of these paths, they are not imported, which is shown in the output of the **show ip bgp vpnv4 vrf vpn-name** command.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when you use the **import ipv4 unicast map** *route-map* command to import an address family from the global table into a VRF. The following sequence of events illustrates how the symptom occurs:

  1. Configure an IP prefix list.
     [example:
     `ip prefix-list COLORADO seq 5 permit 10.1.5.0/24`]
  2. Configure a route map by using the prefix list as the matching criteria.
     [example:
     `route-map UNICAST permit 10 match ip address prefix-list COLORADO`]

3. Import the route map into the VRF.
   [example:

```
ip vrf isp1
   rd 65031:100
   import IPv4 Unicast map UNICAST
   route-target export 65031:100
    route-target import 65031:100]
```

4. Trigger a routing update by entering the **clear ip bgp** command.
5. Check the output of the **show ip bgp vpnv4 vrf vpn-name** command. The output does not show entries from the BGP neighbor.

Workaround: There is no workaround.

- CSCsh17035

  Symptoms: A route may flap continuously and the CPU usage may be high continuously.

  Conditions: This symptom is observed on a Cisco router that is configured with a static route loop.

  Workaround: Do not configure a static route loop.

- CSCsh19852

  Symptoms: When an OSPF interface goes down, some Finite State Machine (FSM) events do not occur. For example, old network LSAs may not be removed by the Designate Router (DR).

  Conditions: This symptom is observed on a Cisco router that runs a Cisco IOS software image that integrates the fix for caveat CSCek63900. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCek63900. 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.

- 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.

- CSCsh65136

  Symptoms: RSVP reservations may become lost or may not be rebuilt when an SSO switchover occurs. Although RSVP is not SSO-aware, RSVP reservations should be re-established after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with dual Supervisor Engine 720 modules and a Policy Feature Card 3BXL (PFC3BXL) and that functions in the following configuration:

  – The Cisco 7600 series functions as a mid-point router.
  – The router that sends RSVP reservations is a downstream router.
  – The router that should receive the RSVP reservations is an upstream router and is enabled for RSVP CAC.

  The interfaces that are used in the topology are Gigabit Ethernet interfaces and 10-Gigabit Ethernet with subinterfaces.

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

- CSCsh66294

  Symptoms: A Cisco 7600 series that is configured for BGP crashes during normal operation.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB and that functions as a PE router in an MPLS environment.

  Workaround: There is no workaround.

- CSCuk58462

  Symptoms: When a route map is configured, routes may not be filtered as you would expect them to be filtered.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that functions in an MPLS VPN environment.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur for redistributed route maps.

ISO CLNS

- CSCse30000

  Symptoms: An L1 LSP that is originated on a local router may not be flooded to its neighbors until the local IS-IS LSP lifetime expires, and the IS-IS floods a new LSP and runs a periodic FSPF.

  Conditions: This symptom is observed on an IS-IS Level 1 - Level 2 (L1L2) router.

  Workaround: Lower the IS-IS LSP lifetime to reduce the period the symptom lasts.

- 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.

- CSCse85158

  Symptoms: Locally advertised networks that are configured for the NSAP address- family under BGP will not be readvertised once they have been cleared from the BGP table.

  Conditions: Once the **clear bgp nsap unicast *** command has been issued, the networks will no longer appear in the output of the **show bgp nsap unicast** command.

  Workaround: There is no workaround.

- CSCse93383

  Symptoms: The default value for the CSNP interval may not be set.

  Conditions: This symptom is observed on a Cisco router when you configure a LAN subinterface to be an ISIS point-to-point subinterface by entering the **isis network point-to-point** command. The default value may remain tho one of the LAN.

  Workaround: Manually configure the CSNP interval.

- CSCsg28497

  Symptoms: An IS-IS adjacency may flap when an RP switchover occurs.

Conditions: This symptom is observed on a Cisco router that is configured for IS-IS Multi-Topology, IS-IS NSF Awareness, and IPv4 and IPv6 unicast.

Workaround: There is no workaround.

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

- CSCeb68312

  Symptoms: When a virtual server is configured to use port 0 and an HTTP probe is configured to use port 80, the HTTP probe does use port 80, but the host tag shows that the HTTP probe uses port 0. Not only is a port number not required in the host tag, the port number of 0 is invalid. This situation may cause problems with Internet Information Services (IIS) 6.0 running on Windows Server 2003.

  Conditions: This symptom is observed on a Cisco platform that is configured for IOS Server Load Balancing (IOS SLB).

  Workaround: Do not configure a virtual server to use port 0 when HTTP probes are used. Rather, configure the virtual server to use a specific port, or use TCP or ICMP probes.

- CSCec12299

  Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

  Workarounds are available to help mitigate this vulnerability.

  This issue is triggered by a logic error when processing extended communities on the PE device.

  This issue cannot be deterministically exploited by an attacker.

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-vpn.shtml.

- 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.

- CSCef25686

  Symptoms: A number of PVCs may become locked in an inactive state, and the following type of error message may appear in the log:

  ```
  %ATM-3-FAILREMOVEVC: ATM failed to remove VC(VCD=X, VPI=X, VCI=X) on Interface ATM X/X/X,
  (Cause of the failure: PVC removal during recreation failed)
  ```

  Conditions: This symptom is observed when you change the parameters of a VC class while the PVC is active and while you view the PVC status in the output of the **show atm vc interface** *interface-number* command.

  The symptom occurs when you change the PVC speed in a VC class via one Telnet (or console) session and you enter the **show atm vc interface** *interface-number* command via another Telnet (or console) session.

  Workaround: To remotely resolve the symptoms, remotely initiate an HA failover or remotely reload the affected router.

- CSCeg03733

  Symptoms: A router may reload because of a memory corruption when you query via getmany or getbulk the entire ciscoCBQosMIB (1.3.6.1.4.1.9.9.166) or when you poll the cbQosQueueingStatsTable or cbQosPoliceStatsTable.

  Conditions: This symptom is observed on a Cisco 7500 series that runs the rsp-jsv-mz image of Cisco IOS interim Release 12.3(11.4) when the following tables in the CBQOSMIB are polled:

  - getREDClassStats
  - getTSStatsEntry
  - getQueueingStatsEntry
  - getPoliceStatsEntry

  The symptom may not be platform-specific.

  Workaround: Do not query the entire ciscoCBQosMIB and do not poll the cbQosQueueingStatsTable or cbQosPoliceStatsTable.

- CSCeh15378

  Symptoms: When you shut down an ATM main interface, the state of the local ATM circuit goes down as expected. However, when you then enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on a subinterface of the same ATM main interface that is shut down, the local circuit state comes back up again, and an "SLI UP" message is sent to a remote PE router.

  Conditions: This symptom is observed on a Cisco router when the subinterface has an Xconnect attachment circuit that is configured for ATM VP Mode.

Workaround: There is no workaround.

- CSCeh41598

  Symptoms: When RIP is enabled and disabled successively 50 to 60 times in a row, the router reloads unexpectedly during the “RIP managed timer” process.

  Conditions: This symptom is observed on a Cisco router that has 15,000 learned RIP prefixes. However, note that RIP does not properly scale beyond about 5000 routes on a high-end router.

  Workaround: Do not enable and disable RIP successively 50 to 60 times in a row.

  First Alternate Workaround: Limit the number of RIP prefixes to 5000 or less.

  Second Alternate Workaround: Before RIP is disabled, for example through the **no router rip** command, remove the network entries under the **router rip** command.

- CSCei23358

  Symptoms: IPv6 prefixes that match the **network** command remain advertised after the **network** command has been disabled.

  Conditions: This symptom is observed when the **network** command is specified within the **address-family ipv6** command for a BGP configuration, and is subsequently removed by entering the **no network** command.

  Workaround: There is no workaround.

- 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.

- CSCek02024

  Symptoms: MNCP negotiations between PE routers fail when cell packing is configured.

  Conditions: This symptom is observed on Cisco routers that function in an L2VPN Pseudowire Switching configuration across Intra-Autonomous Systems and that have VCs that are configured for ATM over MPLS (ATMoMPLS) and Peak Cell Rate (PCR).

  Workaround: There is no workaround. Note that the symptom does not occur when cell packing is not configured.

- CSCek03591

  Symptoms: A traffic class is deleted even when there is traffic that matches the ACL for the traffic class.

  Conditions: This symptom is observed when a subscriber session is configured with a traffic class that is configured with a Layer 4 redirect feature and idle timeout.

  Workaround: There is no workaround.

- CSCek23840

  Symptoms: When a virtual-access interface is invoked, it does not inherit an outbound service policy and a Link Fragmentation and Interleaving (LFI) configuration from the virtual template. Also, 75 percent of the packets are dropped from the interface.

  Conditions: These symptoms are observed on a Cisco router that is configured for MLP.

Workaround: There is no workaround.

- CSCek26931

  Symptoms: A session-based QoS service policy may not be active.

  Conditions: This symptom is observed when a QoS service policy is attached to a PPPoE session that is forwarded. In this situation, the QoS service policy is not automatically attached to the forwarded session and is therefore not active on the forwarded session.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCek37963

  Symptoms: A QoS policy map may fail on ATM, HDLC, and Frame Relay interfaces.

  Conditions: This symptom is observed on a Cisco 7600 series that has a QoS policy map that is configured for WRED with a police action at the first and second level. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur when the QoS policy map is configured for WRED only.

- CSCek39364

  Symptoms: The standby RP reloads when you unconfigure an ATM bundle.

  Conditions: This symptom is observed on a Cisco router when you configure an ATM bundle and PVC bundle and then immediately unconfigure the ATM bundle.

  Workaround: There is no workaround.

- CSCek40394

  Symptoms: The queueing hierarchy is not removed when it should be removed, even though the output of the **show policy-map interface** command indicates that the queueing hierarchy is removed.

  Conditions: This symptom is observed when you detach a service policy that has queueing features in the policy map.

  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.

- CSCek43610

  Symptoms: After you perform an OIR of a line card or SPA, there is no more connectivity and a ping fails.

  Conditions: This symptom is observed on a Cisco 7600 series that is connected back-to-back to another Cisco 7600 series over a single-VLAN BCP on OC-3 POS SPAs that are installed in SIP-400 line cards. The symptom occurs after you have performed an OIR of the SPAs or line cards on both sides.

  Workaround: There is no workaround.

- CSCek43669

  Symptoms: An input policy that is configured for a default-class does not function for a class that is not a queueing class such as a class with a marking policy.

  Conditions: This symptom is observed only on an ATM SPA that is configured for QoS and that is installed in a SIP-200.

  Workaround: There is no workaround.

- CSCek44025

  Symptoms: A router may crash when a hierarchical policy is attached to a Frame Relay PVC.

  Conditions: This symptom is observed on a Cisco router when the following conditions are present:

  – The hierarchical policy has the **shape** command enabled in the class default of the parent policy and has a child policy.
  – The Frame Relay PVC is configured for FRF.12 in a map class.

  Workaround: There is no workaround.

- CSCek44427

  Symptoms: An interface of a T3/E3 serial SPA passes traffic even though the output of the **show controller** command shows that there is a “Loss of Frame” alarm. When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface of the SPA, the alarm is not cleared.

  Conditions: This symptom is observed on a Cisco platform that is configured with a T3/E3 serial SPA.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface at the remote end.

Further Problem Description: The symptom does not affect proper operation of the platform or the traffic. However, the incorrect alarm status may affect network management utilities.

- CSCek44532

  Symptoms: A standby RP may reload repeatedly when you enter the **issu loadversion** command during a period of high checkpointing activity. When you enter the **show checkpoint statistics** command on the active RP, the output shows that the checkpointing IPC flow control status remains set to zero indefinitely:

  ```
  CHKPT FLOW_ON status = 0
  ```

  Conditions: This symptom is observed on a Cisco router when the standby RP reloads as part of the In-Service Software Upgrade (ISSU) process while, for example, a large number of PPPoA sessions are being disconnected.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **issu abortversion** command to cancel the ISSU process, and then reload the router.

- 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.

- CSCek46189

  Symptoms: The forced target-probing functionality in Optimized Edge Routing (OER) may not work as expected.

  Conditions: This symptom is observed only when a policy changes in a configuration in which learned prefixes are deleted and new policies take effect.

  Workaround: There is no workaround.

- CSCek46832

  Symptoms: The following message appears on the console:

  ```
  SEC 8:00:08:11: %TAGCON-3-LCLTAG_ALLOC: Cannot allocate local tag
  ```

  Conditions: This symptom has been observed when dual RPs with SSO and VPLS are configured.

  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.

- 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.

- 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.

- 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.

- CSCek50172

  Symptoms: An Embedded Event Manager (EEM) policy that has the **event interface** command enabled cannot be registered, and a traceback is generated.

  Conditions: This symptom is observed when the **event interface** command has the **poll-interval** keyword enabled and when the *poll-int-value* argument has a value that is larger than 2097151.

  Workaround: Specify a *poll-int-value* argument with a value that is lower than 2097151.

- CSCek51919

  Symptoms: A Cisco router that functions as an Intelligent Service Gateway (ISG) may reload while sessions are being cleared.

  Conditions: This symptom is observed only when the port-bundle host key (PBHK) feature is configured for the sessions.

  Workaround: Do not configure the PBHK feature for the sessions.

- 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.

- CSCek54946

  Symptoms: On a Cisco 7600 series, 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.

- CSCek55001

  Symptoms: A router may crash when you enter the **dir /recursive** command.

  Conditions: This symptom is observed on a router that has a Cisco IOS File System (IFS) and occurs only when 40 subdirectories are created. The symptom does not occur when you enter the **dir** command without the **/recursive** keyword.

  Workaround: When more than 40 subdirectories are created, do not use the **dir /recursive** command. Rather, use the **show disk** command.

- CSCek58360

  Symptoms: The circuit ID and remote ID of option 82 in a DHCP relay reply message may be empty and may cause a DHCP relay reply validation error, resulting in a DHCP lease renewal failure.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when an IP session that is initiated by DHCP involves a VRF transfer.

  Workaround: There is no workaround.

- CSCek58678

  Symptoms: When you attempt to configure an invalid access control list (ACL), the following error message is generated:

  ```
  %SYS-3-INTPRINT: Illegal printing attempt from interrupt level.
  ```

  When the router is configured with a SIP-200, the following message is also generated:

  ```
  SIP200_MP-4-PAUSE: Non-master CPU is suspended for too long.
  ```

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured for Policy Based Routing (PBR).

  Workaround: There is no workaround.

- CSCek60118

  Symptoms: A traceback may be generated when you configure the L2VPN Pseudowire Redundancy feature.

  Conditions: This symptom is observed on a Cisco 7600 series but may be platform-independent.

  Workaround: There is no workaround. However, note that the functionality of the router is not impacted by the traceback.

- 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.

- CSCek63629

  Symptoms: When you first reset the standby RP and then a switchover occurs, the following error message and a traceback are generated:

  ```
  %LFD-3-ORPHANNONIPLTE: Found a non-owned non-IP LTE of ptype 5 - label 0/0.
  ```

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

  Workaround: There is no workaround.

- CSCek64847

  Symptoms: On a router that is configured for Hot Standby Router Protocol (HSRP), the hold timer that is configured via the **standby timers msec** command does not function properly when the standby group number is 17 or higher.

  The configured standby hold time changes unexpectedly to 3 times the group number value instead of remaining in the 50-3000 msec range when the standby group is configured in the 17-4095 range.

  Also, when a relatively high number is configured for the standby group, a "%PARSER-4-BADRANGE" error message is generated.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(6)T3 or Release 12.4(11)T but may also affect other releases such as Release 12.2SR.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.4(5a).

- CSCek65022

  Symptoms: A 7600-SSC-400 SPA services carrier may crash during the boot process of a SPA.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router when an IPsec VPN Shared Port Adapter (SPA-IPSEC-2G) that is installed in the 7600-SSC-400 boots.

Workaround: There is no workaround.

- CSCek66294

  Symptoms: The TCP MSS Adjustment feature works only in the ingress direction. The feature should work both in the ingress and egress direction.

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

  Workaround: There is no workaround.

- CSCek69134

  Symptoms: When you enter the **default interface** command on an interface with a scaled Ethernet Virtual Circuit (EVC) service instance configuration, it may take a long time for the command to be executed, and during this time, the CPU usage of the RP may increase to 100 percent. In addition, many error messages may be generated.

  Conditions: This symptom is observed on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB when a scaled EVC service instance configuration is enabled on a Gigabit Ethernet port of a 20-port Ethernet Services line card (7600-ES20-GE) that is installed in a SIP-400.

  Workaround: There is no workaround. You must wait until the command has been executed. However, the command functions properly.

  Further Problem Description: The **default interface** command is often used to set an interface to its default state before a configuration is applied, and it is used to remove a scaled configuration from an interface by just entering one command rather than deleting individual configuration lines one-by-one.

  As an alternative, you can enter the **no service instance** command for each service instance on the port. The following example shows steps to simplify the process:

  Instead of entering the **default gi1/0/1** command, do the following:

  1. Enter the **show running interface gi1/0/1 | inc service instance** command.
  2. Cut-and-paste the output into your preferred editor.
  3. Edit the file by placing “no” before each line.
  4. Enter the following configuration:

     ```
     conf t
          int gi1/0/1
          <paste the file>
     ```

- CSCin85894

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

  1. Symptom 1: A “%SYS-3-MGDTIMER” error message followed by a traceback may be generated at the “mgd_timer_complain_uninit” function when an extended ACL is configured with the same name as an active reflexive ACL.

     Condition 1: This symptom is observed when the extended ACL is configured with the same name as the reflexive ACL, when the reflexive timer expires at the moment of configuration, and when the dynamic entries of the reflexive ACL are still in place when you configure the extended ACL.

     Workaround 1: Wait until the reflexive timer expires before you configure an extended ACL with same name as a reflexive ACL.

  2. Symptom 2: A software-forced reload may occur when a standard ACL is configured with the same name as an active reflexive ACL.

Condition 2: This symptom is observed when the standard ACL is configured with the same name as the reflexive ACL, when the reflexive timer expires at the moment of configuration, and when the dynamic entries of the reflexive ACL are still in place when you configure the standard ACL.

Workaround 2: Wait until the reflexive timer expires before you configure a standard ACL with same name as a reflexive ACL.

- CSCir00361

  Symptoms: The E1 layer entries for a channelized E3 port adapter may be missing from the IF-MIB list, causing the absence of the corresponding DS1 layer Descriptor and Stack entries when an SNMP walk is performed.

  Conditions: This symptom is observed on a Cisco router that functions in a very simple configuration in which a channelized E3 port adapter is configured with several E1 layers.

  Workaround: There is no workaround.

- CSCir01449

  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 on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRA or Release 12.2(33)SRB when the following conditions are present:

  - The CPU usage is 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: Do not use SSHv2 when the router is very stressed.

- CSCsa54608

  The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition.

  Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.

  Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected.

  Only devices running certain versions of Cisco IOS are affected.

  Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

  This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml.

- CSCsa96960

  Symptoms: MPLS OAM echo request packets may be forwarded from a different interface than the interface that is reported in an MPLS echo reply that is sent in response to an LSP traceroute.

Conditions: This symptom is observed on a Cisco router when an LSP traceroute is sent under the following conditions:

- The penultimate hop has multiple parallel paths, at least one of which has MPLS enabled.
- One or more of the parallel paths have MPLS disabled.

Workaround: Ensure that MPLS is enabled on all equal-cost paths at the penultimate hop.

- CSCsb25404

  Symptoms: The startup configuration in NVRAM is not loaded onto line cards when the router is manually reloaded.

  Conditions: This symptom is observed on a Cisco 12000 series that functions as a multiservice edge (MSE) router when the ATM Cell Relay over MPLS feature is configured on 500 connections. The symptom may also occur on other platforms.

  Workaround: After the router has been reloaded, cut and paste the initially rejected configuration onto the line cards.

- 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.

- 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.

- CSCsb79895

  Symptoms: An authentication check fails for incoming packets. When you enable the **debug ip rip** command, an "invalid authentication" error message is generated.

  Conditions: This symptom is observed on a Cisco router when the RIP routing protocol is configured along with MD5 interface authentication.

  Workaround: There is no workaround.

- 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.

- CSCsb94859

  Symptoms: AToM VCs do not come up after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that is configured with AToM VCs when you perform a soft SSO switchover by entering the **redundancy force-switchover** command, preventing the AToM VCs from coming up on the standby RP and the AToM circuit from being established. Note that the symptom is platform-independent

  Workaround: First, configure an incorrect MTU value on the AToM VCs. Then, change the MTU to the correct value. Doing so brings up the AToM VCs and establishes the AToM circuit.

- CSCsc06891

  Symptoms: There are no traps or notifications send when a compact flash disk is inserted in or removed from device disk0 or disk1.

  When you enter the **show running-config | incl snmp-server enable traps flash snmp-server enable traps flash insertion removal** command, the following output is shown:

  ```
  %FILESYS-SP-5-DEV: PCMCIA flash card removed from disk1
  %FILESYS-SP-5-DEV: PCMCIA flash card inserted into disk1
  ```

  Conditions: This symptom is observed on a Cisco router and switch that are configured with a PCMCIA file system.

  Workaround: There is no workaround.

- 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.

- 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 and Cisco 7600 series that run a native Cisco IOS software image.

  Workaround: There is no workaround.

- CSCsc49134

  Symptoms: A platform may crash when you configure an ATM multipoint subinterface.

  Conditions: This symptom is observed on a Cisco platform when there are already some ATM subinterfaces that are configured for ATM PVC discovery.

  Workaround: There is no workaround.

- 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.

- CSCsc58556

  Symptoms: A Cisco router may crash when an EEM Tcl policy runs.

  Conditions: This symptom is observed when the available memory is very low.

  Workaround: Increase the available memory. If this not an option, there is no workaround.

- 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.

- 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.

- CSCsc72515

  Symptoms: A downstream interface that becomes a non-designated forwarder (DF) interface may not be deleted from the outgoing interface list (olist) for certain (*,G) groups. This situation causes packets to be incorrectly forwarded and leads to looping.

  Conditions: This symptom is observed on a Cisco router that is configured for Bidirectional PIM when a DF interface that forwards traffic downstream changes to a non-DF interface.

  Workaround: There is no workaround.

- CSCsc80303

  Symptoms: IPC Watermark messages may be generated when a trunking interface goes up or down, and a memory leak may occur.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with a dot1q trunking interface that is bundled with more than 2000 VLAN interfaces.

  Workaround: There is no workaround.

- CSCsc94240

  Symptoms: Some line cards may reset when an SSO switchover occurs.

  Conditions: This symptom is observed on a Cisco 7600 series after two or three SSO switchovers have occurred.

  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.

- CSCsd04299

  Symptoms: A router that has a large number of pending sessions may generate a “Memory Low” message.

  Conditions: This symptom is observed on a Cisco router when 32,000 PPPoEoA sessions are brought up simultaneously and occurs because of limited resources while call admission control is not strictly enforced. In this situation, the remote PPPoE software or host software do not respond fast enough.

  Workaround: Do not bring up 32,000 PPPoEoA sessions simultaneously. Rather, bring up the sessions in increments, for example, bring up 10,000 sessions, then another 10,000 sessions, and then the remaining 12,000 sessions.

- 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.

- CSCsd20327

  Symptoms: Web Cache Communication Protocol (WCCP) for service 90 is going up and down on a Cisco router that runs Cisco IOS Release 12.4(3b)B. The router has services 81, 82 and 90 configured. The only service that has a problem is 90. The packet traces indicate that the router is sometimes responding to “Here_I_Am” messages from the cache with “I_See_You” messages that contain an incorrect destination IP address. This situation leads to a loss of WCCP service.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(3b) but may also affect other releases.

  Workaround: There is no workaround.

- CSCsd22712

  Symptoms: A memory leak may occur on a SIP-200 when you perform an OIR of a SPA that is installed in the SIP-200 and that has a large service policy applied at the ATM subinterface level.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router. The amount of memory that leaks depends on the number of subinterfaces to which the service policy is applied and the number of class maps for each service policy.

Workaround: Do not perform an OIR of a SPA that has a relatively large service policy.

- 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.

- CSCsd33837

  Symptoms: The crypto IPsec and IKE SSO clients do not function, preventing the HA redundancy progression sequence from working correctly, and causing the standby RP to reload.

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

  Workaround: There is no workaround.

- CSCsd36608

  Symptoms: A memory leak may occur in the interprocess communications (IPC) when a line card is reset.

  Conditions: This symptom is observed on a Cisco router that is configured for In Service Software Upgrade (ISSU).

  Workaround: There is no workaround.

- CSCsd38693

  Symptoms: Renaming a file to a string that contains multiple trailing dots (“.” characters) corrupts the file system on ATA, CF, and USB flash storage devices.

  Conditions: This symptom is observed when you enter the following commands to rename the file:

  ```
  rename disk0:file2 disk0:file3...
  ```

  Workaround: Avoid renaming a file that contains multiple trailing “.” characters. When the symptom has occurred and the file system is no longer accessible, you must reformat the disk by entering the **format disk0:** command.

- 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.

- 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.

- 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.

- CSCsd50101

  Symptoms: When you enter the **issu loadversion** *active-slot active-image standby-slot standby-image* command, the active RP may crash.

  Conditions: This symptom is observed rarely on a Cisco 10000 series that functions in SSO mode. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCsd68445

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

  1. Symptom 1: You may not be able to apply a QoS policy map with class-based shaping that is configured in the default class on a dot1q subinterface, and the following error messages may be generated:

     Configuring this shaping class will impact guarantees in other classes under this policy-map

     Condition 1: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(27)SBC2 when a hierarchical QoS policy is configured in the following way and when the shape rate is higher than the CIR rate:

     ```
     policy-map child-qos
     class user-defined-class priority
     police cir cir-rate bc Bc be Be
     conform-action transmit
     exceed-action drop

     policy-map parent-qos
     class class-default
     shape average shape-rate
     service-policy child-qos
     ```

     Workaround 1: There is no workaround.

  2. Symptom 2: You may not be able to apply a QoS policy map with class-based shaping that is configured in the default class on a dot1q subinterface, and the following error messages may be generated:

     Configuring this shaping class will impact guarantees in other classes under this policy-map

     Condition 2: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(27)SBC2 when a single policy map with class-based shaping is configured in the following way:

     ```
     policy-map shaping-qos
     class class-default
     shape average shape-rate
     ```

     Workaround 2: Perform the following steps:

     1) Configure a new class map that has the same characteristics as the original class default as in the example below, in which the new class map is called “my-class-default”:

     ```
     class-map match-all my-class-default
     match any
     ```

     2) Configure the new policy map by using the just created class-default equivalent class (“my-class-default”) as following example, in which the new policy map is called “my-policy-map”:

     ```
     policy-map my-policy-map
     class my-class-default
     shape average shape-rate
     ```

     3) Apply the service policy (“my-class-default”) to the dot1q subinterface.

- CSCsd69480

  Symptoms: When links flap on an interface of a PA-MC-STM1 port adapter that is installed in an enhanced FlexWAN module, the following error message may be generated:

  ```
  %HYPERION-4-HYP_RESET: Hyperion Error Interrupt. Resetting ASIC.
  ```

  The output of the **show interface stats** command shows line errors for the flapping line.

Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that run Cisco IOS Release 12.2(17d)SXB9 but may also occur in other releases.

Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCsd76528

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

  1. Symptom 1: None of the policy classes after the first child policy of a hierarchical QoS policy take effect when you reload the router.

     Condition 1: This symptom is observed on a Cisco 7304 that has hierarchical QoS policies with multiple child policies but may also occur on other platforms.

Workaround 1: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **service-policy output** interface configuration command to enable the child policies to take effect. Note that the symptom does not occur for a hierarchical QoS policy with only one child policy in the very last class of the parent policy.

2. Symptom 2: On a Cisco 10000 series that is configured with hierarchical queueing policies, when you remove the **match vlan** command for a VLAN that matches a dot1q subinterface, the queues that are allocated to the subinterface are not cleared, allowing traffic to continue to flow through these queues.

   Condition 2: This symptom is observed on a Cisco 10000 series that has hierarchical QoS policies with multiple child policies but may also occur on other platforms.

   Workaround 2: There is no workaround. Note that the symptom does not occur for a hierarchical QoS policy with only one child policy in the very last class of the parent policy.

- CSCsd77207

  Symptoms: Hardware-switching of bidirectional PIM traffic may not function when a large number of subinterfaces (about 200) are configured via the **copy** command because the existing multicast hardware entries are unexpectedly removed.

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

  Workaround: Do not configure the subinterfaces via the **copy** command. Rather, configure the subinterfaces manually.

- 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.

- CSCsd80745

  Symptoms: A router that is configured for IPSec and ISAKMP may reload unexpectedly because of a bus error exception that is triggered by an address error exception.

  Conditions: This symptom is observed rarely during ISAKMP negotiation when a new IKE SA is being negotiated. The symptom is more likely to occur when low lifetimes are used for IKE and IPSec rekeying.

  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.

- 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.

- CSCsd87844

  Symptoms: When a route distinguisher (RD) that is configured for a VRF is deleted and then reconfigured, the standby RP may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router that has dual RPs that function in HA mode and that is configured for MPLS VPN.

  Workaround: Delete the VRF itself and then reconfigure the VRF in order to change the RD. If this is not an option, there is no workaround.

  Further Problem Description: The symptom occurs because the processing of the **no rd** command is completed only on the active RP only. On the standby RP, the processing does not clear a flag that signals the completion of the processing **no rd** command. Then, when the RD is reconfigured, the configuration succeeds on the active RP but fails on the standby RP, causing the standby RP to reload.

- 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.

- 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.

- CSCsd96436

  Symptoms: Non-aggregate random-detect configurations are accepted in service policies that are applied to interfaces on a SIP-600. However, the SIP-600 supports only aggregate random detect configurations.

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

  Workaround. Remove any non-aggregate random-detect configurations, and only use aggregate random-detect configurations.

- CSCsd97648

  Symptoms: After more than one switchover has occurred on a router that is configured with a source Encapsulated Remote SPAN (ERSPAN) session, the bit rate of the destination port for the source ERSPAN session drops from the expected rate. For example, even though there are 560,000 packets on the monitored port, only 440,000 packets are counted on the ERSPAN destination port.

  Conditions: This symptom is observed on Cisco 7600 series after more that one switchover has occurred without a system reset.

  Workaround: Remove and reconfigure the ERSPAN source session to restore the data rate.

- 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.

- CSCsd98686

  Symptoms: The following error message and traceback may be displayed:

  ```
  %XDR-6-CLIENTISSUBADTXTFM: Failed to xmit_transform message - to slot 6, client CEF
  push, context 0
  -Traceback= 41437E50 4141D584 41432B64 4141D674 41421558 414219DC 41416388 413F4738
  413F4EA0 403E11D0 402652A8 40402AD0 404F23F8 404F23E4
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for SSO and that has dCEF enabled by default. The symptom occurs when you disable dCEF and then re-enable it, for example by entering the no **ip cef** command followed by the **ip cef distributed** command or the **no ip routing** command followed by the **ip routing** command.

  Workaround: There is no workaround.

- 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.

- CSCse00843

  Symptoms: On a router that has an ATM subinterface that is in the “shut” state and that has a PVP that is configured for Xconnect, the standby RP continuously generates the following error message when the router is booted:

  ```
  %CWAN_HA-STDBY-4-IFCFG_PLAYBACK_ERROR: Interface Configuration command 261 playback
  failed for slot 4/1.
  ```

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with dual Supervisor Engine 720 modules. The symptom could also occur on other routers.

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

- 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.

- 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.

- CSCse07011

  Symptoms: After an SSO switchover, traffic may fail on a connection that is configured for Frame Relay-to-Ethernet VLAN Interworking over L2TPv3.

  Conditions: This symptom is observed on a Cisco router that is configured with dual RPs and that functions as a PE router.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCse13736

  Symptoms: On a Cisco platform that has 3000 or more IPv6 multicast streams, drops may occur for some of the streams.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series and Cisco 7600 series that run Cisco IOS Release 12.2(18)SXF2, Release 12.2(33)SRA, or Release 12.2(33)ZW.

  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.

- CSCse17034

  Symptoms: When the **crypto engine slot** command is applied to a subinterface but not to the main interface, the command does not take effect.

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

  Workaround: Enter the **crypto engine slot** command for both the main interface and the subinterface.

- 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.

- CSCse17380

  Symptoms: Buffer exhaustion may occur in an AToM IP interworking scenario.

  Conditions: This symptom is observed rarely on a Cisco 7600 series that functions as a PE router and that receives many ARP requests at a fast rate from a CE router that are processed at the process level. The symptom occurs when the router does not have sufficient buffers available to deal with the ARP requests.

  Workaround: There is no workaround.

- CSCse17960

  Symptoms: A Cisco 7304 that has an NPE-G100 processor may access a bad virtual address and reload unexpectedly.

  Conditions: This symptom is observed when traffic flows to an ATM VC that is configured for MLP with a QoS policy and when the Qos policy has a priority class.

  Workaround: There is no workaround.

- CSCse18146

  Symptoms: A line card may reset unexpectedly when it receives traffic after a switchover of the RP has occurred.

  Conditions: This symptom is observed on a Cisco 7600 series when NBAR is configured on an interface of the line card via the **match protocol** *protocol-name* command that is contained in a policy that is attached to the interface.

  Workaround: Disable NBAR by removing the **match protocol** *protocol-name* command.

- 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.

- 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.

- CSCse19687

  Symptoms: “%SYS-3-CPUHOG” messages may be generated after an RPR+ switchover has occurred.

  Conditions: This symptom is observed on a Cisco router that is configured with 4000 EoMPLS VCs, each of which has a Qos policy applied.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCse23918

  Symptoms: A router may crash when the Pseudowire Redundancy feature is enabled and when a failover occurs from a pseudowire-type link (that is, an AToM link) to an access circuit (that is, a Frame Relay link).

  Conditions: This symptom is observed on a Cisco 7301 and Cisco 7304 when you attempt to unprovision an Xconnect circuit that is configured on a PA-A6 port adapter. The symptom is platform-independent.

  Workaround: There is no workaround.

- CSCse24691

  Symptoms: When MLD snooping is enabled and MLD leaves are sent from the last host in a Layer 2 environment, the MAC entry is not cleared but remains in the MLD snooping table. The port list of the MAC entry does not include the last port that was used but points only to the router.

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

  Workaround: There is no workaround.

  Further Problem Description: As long as the MLD snooping table is not full, the symptom is harmless. (The default size of the MLD snooping table is 32 KB.) When the MLD joins are sent, the port list is automatically populated. When MLD snooping table is full, the traffic to any new groups is flooded to all Layer 2 ports.

- 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.

- CSCse26941

  Symptoms: A Cisco 7304 may reload unexpectedly because of a bus error when you enter the **cef table output-chain build favor convergence-speed** command.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(28)SB. However, the symptom is both platform- and release-independent.

  Workaround: There is no workaround.

- CSCse28172

  Symptoms: RIP routes that point to the dialer interface remain in the routing table when a DSL link goes down. However the routes are removed from the RIP database.

  Conditions: This symptom is observed on a Cisco 877 that runs Cisco IOS Release 12.4(4)T1 or Release 12.4(6)T when the dialer interface is located within a VRF. The symptom is both platform- and release-independent.

  Workaround: Clear the routing table.

- 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.

- 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.

- CSCse33543

  Symptoms: The IKE SA setup may fail when the IKE SA number exceeds 255.

  Conditions: This symptom is observed on a Cisco router that is configured for RSA-Sig as the IKE SA authentication method.

  Workaround: There is no workaround.

- 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.

- 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).

- 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.

- 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.

- CSCse39330

  Symptoms: A router does not boot when you first enter the **secure boot-image** command followed by the **format disk** command and then you use the secure image to attempt to boot the router.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system.

  Workaround: There is no workaround.

- CSCse39956

  Symptoms: When a pseudowire VC that has negotiated to use of the Control Word (that is, Cbit = 1) is followed by another pseudowire VC) that has negotiated to not use the Control Word (i.e., Cbit = 0), the Control Word (CW) may still be prepended to the pseudowire VC that has negotiated to not use the CW. As a result, the disposition router (or tail endpoint) does not expect a CW and cannot decapsulate the VC packet; instead, the packet is dropped at the disposition router as a corrupted packet.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series switch and Cisco 7600 series router that are configured with a SIP-600 and that function in a VPLS environment as egress PE routers.

  Workaround: Ensure that VCs in a VPLS environment do not have a mixture of negotiated CWs (that is, Cbits). The output of the **show mpls l2transport binding** command shows the VCs and Cbits.

Further Problem Description: One scenario in which the symptom occurs is the following:

  - A VPLS hub-spoke environment is created with a mixture of hardware-based and software-based EoMPLS VCs.
  - When the SIP-600 detects the CW setting for one VC, it assumes that the VC that follows the first VC also has the CW, and inserts the CW.
  - When a hardware-based EoMPLS VC is in the middle of the replication chain, ping failures may occur for CE routers that are located behind the hardware-based EoMPLS VC. A hardware-based EoMPLS VC does not support the CW and ping failures occur because the MAC address of the customer becomes corrupted.

- CSCse41366

  Symptoms: A ping between two CE routers may fail.

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

  When the symptom occurs, the outputs of the **show mpls l2 vc detail** and **show ssm segment id** commands may show that the connection between the CE routers is up, but the output of the **show sss session** command does not show a session between the CE routers.

  Workaround: There is no workaround.

- 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.

- CSCse45322

  Symptoms: When a tunnel is configured for Path MTU discovery, the configuration may not be propagated from the RP to an IPSec VSA SPA, preventing Path MTU discovery from functioning.

  Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router and may occur when a tunnel is configured for the first time after a reboot.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the tunnel interface to force the configuration to be properly propagated to the IPSec VSA SPA.

  Alternate Workaround: Remove and add back the Path MTU discovery configuration.

- 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.

- 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.

- CSCse51721

  Symptoms: Counters do not increment when you run the CISCO-SONET-MIB. However, when you enter the **show controllers sonet** command, the counters show properly.

  Conditions: This symptom is observed on a Cisco 7600 series that is configured with a channelized STM-1 SPA (SPA-1xCHSTM1/OC3) that receives error packets.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCse62370

  Symptoms: A router may crash when you attach a map class to a Frame Relay data-link connection identifier (DLCI) interface.

  Conditions: This symptom is observed on a Cisco router that is configured with an output policy with Frame Relay Traffic Shaping.

  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.

- 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.

- 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.

- 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.

- 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.

- CSCse75904

  Symptoms: RADIUS accounting updates may still be sent periodically for users that have already disconnected.

  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.

  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.

- 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.

- CSCse77758

  Symptoms: The secondary RP may fail to boot (that is, reach the SSO mode) after the **ipv6 unicast-routing** command is disabled on the primary RP. During the reboot of the secondary RP, the following message is displayed on its console:

  ```
  %Cannot disable IPv6 CEF on this platform
  ```

  On the primary RP, the following messages are displayed on its console:

  ```
  Config Sync: Starting lines from PRC file: -no ipv6 cef
  Config Sync: Bulk-sync failure, Reloading Standby
  ```

  Conditions: This symptom is observed on a Cisco router that has dual RPs and that runs Cisco IOS Release 12.2SB.

  Workaround: First, re-enable IPv6 by entering the **ipv6 unicast-routing** command on the primary RP. Then, reboot the secondary RP.

- 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.

- CSCse78568

  Symptoms: The standby RP resets continuously while loading a large configuration.

  Conditions: This symptom is observed on a Cisco 10000 series but is platform-independent.

  Workaround: There is no workaround.

- CSCse80519

  Symptoms: A router may reload when it receives an extensible markup language (XML) file.

  Conditions: This symptom is observed on a Cisco router that is configured for CNS and occurs when an XML namespace in the operation tag is being declared.

  Workaround: There is no workaround.

- 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.

- CSCse86477

  Symptoms: A router crashes when you detach a map class from a Frame Relay DLCI interface.

  Conditions: This symptom is observed on a Cisco router that is configured with an output policy with Frame Relay traffic shaping.

  Workaround: There is no workaround.

- CSCse86912

  Symptoms: Packets are not switched.

  Conditions: This symptom is observed when you configure a VLAN for Xconnect.

  Workaround: There is no workaround.

- CSCse89636

  Symptoms: The following error messages and tracebacks are generated on a PRE-3 when an In-Service Upgrade (ISU) upgrade (that is, a hardware upgrade) occurs from a PRE-2 that runs Cisco IOS Release 12.2(27)SBB5 to a PRE-3 that runs Cisco IOS Release 12.2(31)SB:

  ```
  %LFD-3-INVINSTALLER: Wrong installer 4 for packet 0/0 update (was 1)
  %LSD-3-LABEL: can't create rewrite for label=0
  ```

  Conditions: This symptom is observed on a Cisco 10000 series but could occur on any platform when you perform an ISU switchover.

  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.

- CSCse90702

  Symptoms: A Frame Relay map may not be established after you perform an OIR of a line card.

  Conditions: This symptom is observed on a Cisco 7600 series when the line card is configured with an MFR bundle.

  Workaround: Create a static Frame Relay map.

  Alternate Workaround: Perform an OIR at both ends simultaneously.

- CSCse91107

  Symptoms: NSF does not function properly for VPN traffic, causing packet loss. This situation can be verified in the output of the **show ip bgp vpnv4 all labels** command.

  Conditions: This symptom is observed on an MPLS PE router after an ISSU upgrade.

  Workaround: There is no workaround.

- CSCse91675

  Symptoms: The RP may generate an “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.

- 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.

- 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.

- CSCse98404

  Symptoms: When you apply an input service policy to an AToM PVC, a router may reload and generate the following error message and traceback:

  ```
  Unexpected exception to CPUvector 300, PC = 119B6D0
  -Traceback= 119B6D0 118E2F8 5952270 118FDC4 11B7680 11B78EC 236988 24BDD4 2E95CC
  ```

  Conditions: This symptom is observed on a Cisco 12000 series that runs Cisco IOS Release 12.0(32)S3 but is platform- and release-independent. The symptom occurs when you enter the following commands:

  ```
  Router(config)#interface x/y.z point-to-point
  Router(config-subif)# no ip directed-broadcast
  Router(config-subif)# no atm enable-ilmi-trap
  Router(config-subif)# pvc a/b l2transport
  Router(cfg-if-atm-l2trans-pvc)# encapsulation aal5
  Router(cfg-if-atm-l2trans-pvc)# xconnect a.b.c.d xy encapsulation mpls
  Router(cfg-if-atm-l2trans-pvc-xconn)#
  Router(cfg-if-atm-l2trans-pvc-xconn)#service-policy test
  ```

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCsf04530

  Symptoms: L2TP may be unable to establish a control channel.

  Conditions: This symptom is observed on a Cisco router that connects to a third-party vendor router that conforms to IETF standards but not to Cisco Attribute-Value Pairs (AVPs).

  Workaround: There is no workaround.

- 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-20080609-snmpv3.shtml

- 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.

- 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.

- CSCsf09186

  Symptoms: When you enter the **show ip route** command to check on the installed routes, the output does not show the routes that have been installed by the RIP.

  Conditions: This symptom is observed on a Cisco router when redistribution is enabled under the RIP.

  Workaround: There is no workaround.

- CSCsf11182

  Symptoms: The output of the **show policy-map interface** *interface-name* **vp** *vpi* **input** command for an ATM interface does not show anything and states that the policy is not configured. However, the output of the **show running-config** command does show the service policy for the ATM interface.

  Conditions: This symptom is observed on a Cisco router after an RP switchover has occurred twice.

  Workaround: There is no workaround.

- 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.

- CSCsf11937

  Symptoms: When you enter the **cd .../.../** command followed by a sequence of **mkdir** commands, the disk becomes corrupt.

  Note that for the **cd .../.../** command, ".../.../" are the arguments, that is, the arguments consist of more than two dots.

  Conditions: This symptom is observed on a Cisco router that has an ATA file system.

  Workaround: Enter the **format** command for the file system.

- 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.

- CSCsf13044

  Symptoms: The outgoing interface (OIF) for bidirectional PIM multicast routes is not updated properly because PIM joins are not received through the MDT tunnel.

  Conditions: This symptom is observed on a Cisco 7600 series that has Gigabit Ethernet interfaces that are configured for dCEF.

  Workaround: There is no workaround.

- 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.

- CSCsf15429

  Symptoms: When you perform an OIR of an OC-3 POS line card, continuous "FR Broadcast Output" error messages may be generated, first causing a CPUHOG condition, and then causing the router to crash.

  Conditions: This symptom is observed on a Cisco 7304. However, the symptom is platform-independent and is related to the Forwarding Information Base (FIB).

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsf27677

  Symptoms: When you perform an In-Service Upgrade (ISU) upgrade (that is, a hardware upgrade) from a PRE-2 to a PRE-3, the Cisco 10000 series may crash and generate the following error message:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x40378AAC-
  ```

  Conditions: This symptom is observed on a Cisco 10000 series but may occur on any platform when you perform an ISU. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl? bugid=CSCse89636. 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.

- CSCsf30618

  Symptoms: A DHCP route is unexpectedly removed for an unnumbered DHCP binding.

  Conditions: This symptom is observed when a DHCP address is renewed.

  Workaround: There is no workaround. However, during the next DHCP address renewal, the DHCP route is added back.

- CSCsf96069

  Symptoms: IPv6 traffic that is processed on MFR interfaces may not be switched via dCEF.

  Conditions: This symptom is observed on a Cisco 7500 series and Cisco 7600 series.

  Workaround: There is no workaround.

- CSCsf96476

  Symptoms: Bidirectional Forwarding Detection may not function properly.

Conditions: This symptom is observed on a Cisco platform that is not MIPS-based such as a Cisco 7600 series and Cisco 12000 series.

Workaround: There is no workaround.

- 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.

- CSCsf98858

  Symptoms: Failure detection time with Bidirectional Forwarding Detection (BFD) echo mode takes longer than with BFD asynchronous mode.

  Conditions: This symptom is observed on a Cisco router that has 100 BFD neighbors.

  Workaround: Use the BFD asynchronous mode by entering the **no bfd echo** command on the interface that has BFD enabled.

- CSCsg02241

  Symptoms: Incorrect NAT translation may occur for one or more faulty Multi-Layer 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.

  Workaround: There is no workaround.

- CSCsg02387

  Symptoms: A time-out occurs when you enter an SNMP command for an IPv6 interface. However, you can ping the IPv6 interface.

  Conditions: This symptom is observed on a Cisco 7200 series but is platform-independent.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- 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.

- CSCsg13828

  Symptoms: A router that is configured for Embedded Event Manager (EEM) may reload unexpectedly.

  Conditions: This symptom is observed when an EMM policy is configured with an event timer or with an action to log output to the console.

  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.

- 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.

- CSCsg17790

  Symptoms: MPLS traffic may be dropped for a few seconds during an RP switchover.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS LDP and occurs because of a timing issue.

  Workaround: There is no workaround.

- CSCsg17957

  Symptoms: A router may crash when forwarding an IP fragment.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(28)SB3 and that is configured for L2TP and QoS. Note that the symptom is not release-specific.

  Workaround: Remove the QoS configuration. If this is not an option, there is no workaround.

- CSCsg18933

  Symptoms: A RIP route is learned from a RIP neighbor via a dialer interface (or other virtual interface type). When the neighbor disconnects and the interface goes down, the RIP route is removed from the RIP database. However, the RIP route remains in the routing table.

  Conditions:

  - RIP is configured with the **no validate-update-source** command.
  - RIP routes are learned via a virtual interface.
  - The virtual interface is using a negotiated address.
  - The problem is platform-independent.

  Workaround: Use the **clear ip route** command to remove the affected routes from the routing table.

- 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.

- CSCsg22369

  Symptoms: In an MPLS TE Fast ReRoute (FRR) environment, when a protected link flaps, all primary LSPs that traverse the link and that are protected by a backup tunnel are reoptimized, that is the old active LSPs are replaced with new LSP.

  For primary TE tunnels without any bandwidth such as primary auto-tunnels, the new LSP is protected by a suitable NHOP or NNHOP backup tunnel, but when this backup tunnel goes for some reason, the new primary LSP is not re-evaluated and moved off the backup tunnel. However, the FRR state continues to shows as “Ready”.

Conditions: This symptom is observed on a Cisco router that functions as an MPLS TE FRR Point of Local Repair (PLR) when the following conditions are present:

  - One or more fast-reroutable primary TE tunnels with zero-bandwidth traverse the PLR.
  - A flap of the protected link occurs.
  - An event occurs that requires the LSP for the backup tunnel (that protects the primary TE LSP) to be torn down.

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.

- 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.

- 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.

- 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.

- CSCsg36982

  Symptoms: A static route is not removed when you enter the **clear ip dhcp binding** command.

  Conditions: This symptom is observed on a Cisco router when the DHCP binding and route are loaded from a database agent.

  Workaround: Do not use a database agent for the restoration of a binding and router.

- 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).

- CSCsg40391

  Symptoms: When a dot1x port is authenticated and assigned a VLAN by an AAA server and then the line card for the port is reset, the assigned VLAN becomes the configured access VLAN for the port. You can see this situation in the running configuration for the port.

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

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, reconfigure the access VLAN for the port to the old value.

  Further Problem Description: If, at a later time, you unconfigure dot1x on the port but do not unconfigure the access VLAN, the configuration for the assigned VLAN remains in place, causing the port to have access to whatever VLAN was previously assigned.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsg51811

  Symptoms: When the OER BGP Inbound Optimization feature is configured and when route control is enforced, route control does not prepend autonomous systems or communities. Rather, router control prepends the same autonomous systems or communities to all external OER interfaces.

Conditions: This symptom is observed on a Cisco router when OER manages inside prefixes that are either learned or configured.

Workaround: There is no workaround.

- CSCsg60791

  Symptoms: The **show oer master appl** command may terminate prematurely, and the following error message is generated:

  Show buffer max size reached

  Conditions: This symptom is observed when there are more than 50 application traffic classes. The command displays only approximately the first 50 application traffic classes.

  Workaround: Based on the type of application traffic class that is configured, use one of the following commands to show the application traffic classes:

  - The output of the **show oer master appl access-list** *name* command shows all applications that are defined in the access list.
  - The output of the **show oer master appl tcp** command shows all applications that use TCP.
  - The output of the **show oer master appl udp** command shows all applications that use UDP.
  - The output of the **show oer master appl** *protocol-number* command shows all applications that use the protocol number that is defined in the *protocol-number* argument.

- CSCsg67551

  Symptoms: LDP sessions flap after a switchover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PE router and that is configured for EIGRP and BGP. Note that the symptom is platform-independent.

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

- 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.

- CSCsg72398

  Symptoms: Traffic to a Cisco IOS SLB virtual server that is configured for UDP may be process-switched.

Conditions: This symptom is observed on a Cisco Catalyst 6000 series switch and Cisco 7600 series router that are configured with multiple virtual servers.

Workaround: Enter the **mls ip slb search wildcard rp** command.

- 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.

- 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.

- 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.

- CSCsg99996

  Symptoms: When an ERP timer event occurs for a particular endpoint, the endpoint may become stuck in a continuous loop.

  Conditions: This symptom is observed on a Cisco router that is configured for High Availability (HA) In-Service Software Upgrade (ISSU).

  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.

- CSCsh12760

  Symptoms: Invalid SPI messages are generated on a remote peer.

  Conditions: This symptom is observed when IPsec rekeying occurs on a Cisco 7600 series that has an IPsec VPN SPA (SPA-IPSEC-2G) and that is connected to a remote peer. The symptom is more likely to occur when there are duplicate SAs and/or dynamic crypto maps.

  Workaround: There is no workaround.

- CSCsh13291

  Symptoms: When a fatal CEF error occurs on a line card other than the RP, CEF becomes disabled on the RP and therefore on the router.

  Conditions: This symptom is observed on a Cisco router after at least one switchover has occurred since the router booted.

  Workaround: There is no workaround.

  Further Problem Description: Another issue can trigger the symptoms: When two 7600-SSC-400 line cards are present in a Cisco 7600 series, CEF on the active RP disables itself about 100 minutes after the router has booted if one or more switchovers have occurred during these 100 minutes.

- 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.

- 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.

- CSCsh26382

  Symptoms: IPsec SAs may be unexpectedly deleted.

  Conditions: This symptom is observed on a Cisco router when the transform set that is used to create IPsec tunnels is a combination of both AH and ESP protocols.

  Workaround: Do not use a combination of AH and ESP protocols for the transform set. Use either the AH protocol or use the ESP protocol.

- CSCsh42857

  Symptoms: After a TE tunnel has been reoptimized, AToM traffic may no longer pass through because the outgoing label and outgoing interface are not updated in the hardware.

  Conditions: This symptom is observed on a Cisco 7600 series that has AToM circuits configured over a TE tunnel that connects to a CE router.

  Temporary Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the interface that faces the CE router or configure and deconfigure the **xconnect** command on the interface that faces the CE router. Doing so re-establishes traffic forwarding until a new reoptimization occurs.

- CSCsh61393

  Symptoms: When the standby supervisor engine becomes active after an RPR+ switchover has occurred, the transmission of all traffic stops.

  Conditions: This symptom is observed on a Cisco 7600 series that functions in an EoMPLS environment. The symptom occurs because a VRF-VLAN with an explicit null label is not properly programmed on the SP and DFC after the standby supervisor engine has become active. This situation can be seen in the output of the following commands:

  On the RP:

  Enter the **show mls cef mpls detail labels** *value* command. For the *value* argument, enter the VRF-VLAN with the explicit null label.

  On the SP:

  – Enter the **show mls cef mpls detail labels** *value* command. For the *value* argument, enter the VRF-VLAN with the explicit null label.

  – Then, enter the **show mls cef adjacency entry** *index* command. For the *index* argument, enter the adjacency index shown in the output of the **show mls cef mpls detail labels** *value* command.

  Workaround: There is no workaround.

- CSCsh66675

  Symptoms: When Circuit Emulation circuits are configured in a very short period via a script and then an RPR+ switchover occurs, the interface of a Circuit Emulation over Packet (CEoP) SPA may shut down.

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

  Workaround: After the RPR+ switchover has occurred, enter the **no shutdown** interface configuration command on the interface of the CEoP SPA.

- CSCsh66793

  Symptoms: After you have performed an OIR of a line card, the number of queues that correspond to QoS policies are smaller than before the OIR because not all queues are recreated.

  Conditions: This symptom is observed on a Cisco 7600 series that has a large number of Ethernet Virtual Circuit (EVC) instances on which QoS policies are configured and that are spread across several interfaces.

  Workaround: Perform another OIR of the line 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.

- CSCuk60910

  Symptoms: A Cisco IOS router may detect a memory corruption and reload.

  Conditions: An interface on the system must be configured for Van Jacobsen TCP header compression, using the **ip tcp header-compression** command, and connected to a third party system.

Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCee73956

  Symptoms: The Generalized TTL Security Mechanism (GTSM), formerly known as BGP TTL Security Hack (BTSH), checks the time-to-live (TTL) value of the packets at the application level, which is not efficient. Also, GTSM does not stop the establishment of a TCP connection for a packet with an invalid TTL value.

  Conditions: This symptom is observed on a Cisco platform that has the **neighbor** *neighbor-address* **security ttl hops** *hop-count* command configured in a BGP environment.

  Workaround: There is no workaround.

- 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.

- 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

- CSCeh64479

  Symptoms: A router reloads unexpectedly when an apparent Layer Two Forwarding (L2F) packet is received.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for Virtual Private Dialup Network (VPDN). However, the symptom is not platform-specific.

  Workaround: There is no workaround.

- 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.

- CSCek31227

  Symptoms: A router may crash when a PPP access circuit flaps repeatedly.

  Conditions: This symptom is observed on a Cisco router that functions in a Virtual Private Dialup Network (VPDN).

  Workaround: There is no workaround.

- 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.

- CSCir00712

  Symptoms: When a LAC receives fragmented data traffic over an L2TP tunnel, the IP layer reassembles the packets and routes them over the wrong interface instead of processing them locally.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(14)T when fragmented L2TP data traffic is received on the LAC from the LNS over the L2TP tunnel. The symptom is release-independent.

  Workaround: There is no workaround.

- CSCsd21476

  Symptoms: A router crashes when you attempt to delete a Frame Relay-to-Ethernet connection.

Conditions: This symptom is observed when you first remove the Frame Relay interface via an OIR and then you attempt to delete the Frame Relay-to-Ethernet connection.

Workaround: Re-insert the Frame Relay interface before attempt to delete the Frame Relay-to-Ethernet connection.

- CSCsf03371

  Symptoms: A router may crash after more than 260,000 PPPoX sessions have flapped.

  Conditions: This symptom is observed on a Cisco router when the **aaa new-model** command is disabled.

  Workaround: Enter the **aaa new-model** command.

- CSCsf28443

  Symptoms: L2TP tunnels may not come up. When this situation occurs, a traceback is generated.

  Conditions: This symptom is observed on a Cisco router that has the **l2tp tunnel timeout no-session never** VPDN group configuration command enabled.

  Workaround: Do not configure the **never** keyword in the command. Rather, enter a value for the *seconds* argument.

- CSCsf28839

  Symptoms: When you change the encapsulation from Frame Relay to another type, a spurious memory access and tracebacks are generated.

  Conditions: This symptom is observed on a Cisco router that has the **encapsulation frame-relay** command enabled on a serial interface when you assign the serial interface to an MFR interface, which causes the Frame Relay encapsulation to be removed from the serial interface.

  Workaround: There is no workaround.

- CSCsg11708

  Symptoms: After An SSO switchover has occurred, punt adjacencies are installed for PPP, causing packets to be process-switched on the RP.

  Conditions: This symptom is observed on a Cisco 7600 series but may not be platform-specific.

  Workaround: Force the interface to reset by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCsg24778

  Symptoms: A router may crash because of a corrupted memory pointer.

  Conditions: This symptom is observed on a Cisco router that is configured for PPPoE Relay and VPDN.

  Workaround: There is no workaround.

- 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.

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