Caveats for Cisco IOS Release 12.2(28)SB through 12.2(31)SB14

Caveats

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 12.2SB is based on Cisco IOS Release 12.2, many caveats that apply to Cisco IOS Release 12.2 also apply to Cisco IOS Release 12.2SB. 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.)

This section consists of the following subsections:

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

Resolved Caveats—Cisco IOS Release 12.2(31)SB14

Cisco IOS Release 12.2(31)SB14 is a rebuild release for Cisco IOS Release 12.2(31)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB14 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCds79402

  Symptoms: Using the **output-delay** router configuration command may affect the rate at which incoming Routing Information Protocol (RIP) updates are processed.

Conditions: To diagnose this situation, look at the output of the **show ip socket** command and look at the IN column for port 520. The value should remain relatively low (less than 20) if the updates are being serviced correctly.

Workaround: Set the **output-delay** router configuration command to a smaller value or remove it altogether.

- CSCec00268

  Symptoms: A multilink interface may stop processing received packets.

  Conditions: This symptom is observed on a Cisco 7500 series when Multilink PPP (MLP) is configured and when a lot of traffic is forwarded to the process-switching path.

  Workaround: To clear the symptom, move the physical interfaces to a new multilink interface with a new interface number.

- 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.

- CSCec85585

  Symptoms: Some virtual circuit (VC) information is missing in the Simple Network Management Protocol (SNMP) MIB object cAal5VccEntry from the output of the **snmpwalk** router configuration command. The ATM VCs 0/100, 0/200 and 0/500 exist on the router but are missing in the MIB.

  Conditions: This symptom is observed on a Cisco 7513 router that is running a special image of Cisco IOS Release 12.2(15)T5. The symptom may also occur in other releases.

  Workaround: Enter the **show atm vc** privileged EXEC command on the same device to obtain a complete list of all the VCs.

- CSCeg80842

  Symptoms: The output of serial interfaces on a PA-MC-8TE1 may become stuck after several days of proper operation.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.3(10a) and that has MLP configured on the serial interfaces of the PA-MC-8TE1.

  Temporary Workaround: Perform an OIR of the PA-MC-8TE1 or reload the router until the symptom occurs again.

  Further Problem Description: The symptom occurs during normal operation of the router. If many errors occur on the link, the symptom is more likely to occur.

- CSCei55605

  Symptoms: The **show kron schedule** command may cause the router to reload.

  Conditions: This symptom is observed when Kron is configured with the occurrence scheduled for Sunday.

  Workaround: Do not issue the **show kron schedule** command.

- CSCek54959

  Symptoms: During switchover following error message appears:

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

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

Workaround: There is no workaround.

- 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.

- CSCek69242

  Symptoms: Even though the interface is not congested, packets are getting dropped on ATM interfaces.

  Conditions: The symptom is observed with Voice Activity Detection (VAD) and the G711 codec.

  Workaround: Do not set the vectors and queueing algorithm if it is already set to QUEUE_PER_VC. The drivers are expected to initialize this if the particular driver supports Per-VC queueing.

  Further Problem Description: ATM drivers now support Per-VC queueing. It sets the idb->queuing_algorithm to QUEUE_PER_VC. But HQF overwrites this to QUEUE_HQF. In many places, including common code, it checks for the queueing algorithm and does ATM Per-VC specific queueing. But since HQF was setting this wrongly, it goes to a separate code.

- CSCek74277

  Symptoms: Back-to-back link goes down in POT1E1 and PA on configuring ISIS.

  Conditions: This symptom happens only in Cisco IOS Release 12.2SR.

  Workaround: There is no workaround.

- CSCsb97913

  Symptoms: The following error messages may be displayed on the active RSP of a Cisco 7500 series:

  ```
  %IPC-3-ISSU_ERROR: ISSU register peer failed with error code 0 for seat 1010000
  %ISSU-3-NOT_FIND_UNDER_ENDPOINT:
  Can not find peer uid by transport ERP id(0x1010000) control block under endpoint.
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that runs a crypto image of Cisco IOS Release 12.2SB.

  Workaround: There is no workaround. Note that the symptom does not cause any side effects.

- CSCsc66612

  Symptoms: A Cisco router configured for Virtual Private Dialup Network (VPDN) may unexpectedly reload with Bus Error.

  Conditions: This symptom was observed on a Cisco7200VXR series router equipped with NPE-G1 processor card running Cisco IOS Release 12.3(14)T3.

  Workaround: There is no workaround.

  Further Problem Description: The crash was preceded by “SYS-2-INPUT_GETBUF: Bad getbuffer” error messages.

- CSCsd36670

  Symptoms: CDP may not be enabled with snmpset.

  Conditions: The symptom is observed when CDP is globally disabled and when the user attempts to enable CDP from SNMP.

Workaround: Enable CDP from CLI.

- CSCse02510

  Symptoms: On a Cisco router that is configured for Hierarchal Queueing 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.

- CSCse03637

  Symptoms: PIM dense mode interoperability issues are seen with Cisco and third party boxes.

  Condition: 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.

- 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.

- CSCse23950

  Symptoms: A router hangs on a regular basis producing the following traceback:

```
%SYS-2-NOTQ: unqueue didn't find 0 in queue 82E19A74
-Process= "<interrupt level>", ipl= 2
-Traceback= 0x80836CE8 0x814DC7F0 0x814EBE5C 0x816DF1F0 0x816DF2A8 0x816DEF74
0x816DE8D4 0x80076750 0x8072CFA0 0x8072D10C 0x803B128C 0x80143E5C 0x801383B4
0x8013AB0C 0x8013D6E0 0x8037DF44
```

  Conditions: This symptom is observed on a router that is acting as an EzVPN Client. From the traceback, it seems that the BVI interface is involved in the crash.

  Workaround: Disable bridging or HW encryption.

- CSCse42370

  Symptoms: Tracebacks are seen while applying queueing policy after deleting/creating subinterfaces.

  Conditions: Tracebacks are seen while applying queueing policy after deleting/creating subinterfaces.

  Workaround: There is no workaround.

- CSCse89897

  Symptoms: The following error messages may be seen:

```
%QOS-3-HQFPOOLERR: interface GigabitEthernet0/2: failed to allocate hqf particle
%QOS-3-HQFPOOLERR: interface GigabitEthernet0/2: failed to allocate hqf particle
%SYS-3-CPUHOG: Task is running for (2004)msecs, more than (2000)msecs
(154/17),process = Logger.
-Traceback= 609222CC 60922360 60920BA4 60766C0C 60765CE8 607663F0 60768328 :
```

```
%SYS-3-CPUHOG: Task is running for (4004)msecs, more than (2000)msecs
(290/17),process = Logger.
-Traceback= 609222CC 60922360 60920BA4 60766C0C 60765CE8 607663F0 60768328
```

Conditions: The symptom is observed with a Cisco 7200 series router with NPE- G1 that is running the c7200-g9js-mz.2006-07-24.XNTD image and is loaded with mixed traffic of IPv6 multicast, IPv6 unicast, SBC RTP, and PPPoE.

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.

- CSCsg39977

  Symptoms: When dialer interfaces are used in conjunction with Multilink PPP (MLP), a router may crash because of a corrupted program counter.

  Conditions: This symptom is observed on a Cisco router when a dialer interface, including interfaces such as ISDN BRI and PRI interfaces, is configured to use MLP and when the queueing mode on the dialer interface is configured for Weighted Fair Queueing (WFQ). Note that WFQ is the default for some types of dialer interfaces.

  Workaround: There is no workaround.

- CSCsh13493

  Symptoms: A router may crash when the standby RP does not enter the Hot Standby state.

  Conditions: This symptom is observed on a Cisco router that functions in a high availability environment during the boot process of the router.

  Workaround: There is no workaround.

- CSCsi06948

  Symptoms: A device crashes with a bus error when the **show ip bgp dampening dampened-paths** command is used.

  Conditions: This symptom is observed when the **show ip bgp dampening dampened-paths** command is used and the device is at the "More" prompt to continue with remaining output, if the BGP session goes down at that time (for example, receiving a notification) or because of a **clear ip bgp** command from another vty.

  Workaround: There is no workaround.

  If dampening is configured, do not run "sh ip bgp neighbors <x.x.x.x> dampened-routes" "sh ip bgp dampening dampened-paths" which can cause this problem

- CSCsi48276

  Symptoms: A spurious access occurs when a serial port adapter is removed via Online Insertion and Removal (OIR).

Conditions: This symptom is observed if one or more serial interfaces on the port adapter are members of a multilink bundle and data traffic is flowing through the bundle when the port adapter is removed. This symptom has been seen on a Cisco 7200 series router, but it is not believed to be platform-specific.

Workaround: Shut down the serial interfaces before removing the port adapter.

- 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.

- CSCsi63075

  Symptoms: The removal of NAT protocol address translation command from the configuration, which refers to the same interface which is used for overloading, will cause a system restart.

  Conditions: This symptom occurs assuming that the interface used for overloading/PAT has an IP address:

  ```
  ip nat inside source route-map <name> interface Ethernet1/0 overload
  ip nat inside source static tcp <addr> <lport> interface Ethernet1/0 <gport>
  no ip nat inside source static tcp <addr> <lport> interface Ethernet1/0 <gport>
  ```

  This is applicable for all Cisco IOS 12.2S based releases.

  Workaround: Do not remove the PAT configuration once applied.

- CSCsi94859

  Symptoms: A PE router crashes when ATM PVC is created on the other end CE.

  Conditions: This symptom occurs when an ethernet sub-interface bound to an ATM VC through a **connect** command is deleted, ATM VC gets improperly removed leading to stray VCD in the PA. When traffic passes through the stray ATM VC, it crashes.

  Workaround: Do not remove ethernet subinterface when it is bound to an ATM VC through a **connect** command.

- CSCsj10933

  Symptoms: Under extremely unusual conditions, a multilink-group interface may not start PPP, after two or more serial links have negotiated PPP and joined that bundle interface, creating a bundle. Inspection of the output from the **show ppp multilink** command will show that the bundle exists and has active member links. However, inspection of output from **show interface** and **show ppp interface** will reveal that the bundle interface is in a “Line-Protocol Down” state, and further indicates that the bundle interface is in “LCP Negotiating” phase.

  Conditions: This can occur if two or more PPP serial links are assigned to a common multilink-group interface, and the links come up and negotiate PPP in near perfect simultaneity, but the links do not receive the exact same remote endpoint identification credentials (these being the PPP Multilink Endpoint Discriminator and/or PPP Authenticated username) on all the links. Note that this situation should never normally arise, at it could not itself occur except as a result of some other error (for example a cabling error, a misconfiguration at one end or the other, or an operational error with the remote system). It is implicit in being assigned to a single group interface that all links in the set will be providing identical identification information.

  Workaround: Any sequence which resets the bundle interface will generally clear the condition. For example, **clear interface** *Multilink10*.

Further Problem Description: This situation occurs if a link comes up and starts the formation of a bundle, and then a second link comes up - with conflicting identification information - in the window of time between when the first link starts the formation of the bundle and when that formation can be completed. Also note that this is specific to the use of static bundle interfaces (multilink group interfaces), and not an issue when dynamic (virtual-access) interfaces are used for the bundles.

- 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.

  Impacts: May impact traffic forwarding.

  Workaround: There is no workaround.

- CSCsj54606

  Symptoms: Invalid updates to the system clock are allowed on the Cisco IOS command line interface (CLI).

  Conditions: The symptoms are observed when a user attempts to configure the set end of summer-time earlier than the start of summer-time:

```
Router(config)#clock summer-time PDT date 11 mar 2007 2:00 ?
  <1-31>  Date to end
  MONTH   Month to end

Router(config)#$r-time PDT date 11 mar 2007 2:00 11 march 2007 00:00 60
```

  Workaround: Do not pass invalid arguments to the **clock summer- time** command on the Cisco IOS CLI.

- CSCsj71998

  Symptoms: An ATM interface loses its assigned IP address if the interface is gracefully stopped/started.

  Condition: This symptom is observed in Cisco IOS Release 12.4(17).

  Workaround: Reconfigure the interface.

- CSCsj83966

  Symptoms: There may be a CPU HOG due to “Syslog Traps” message seen on a device.

  Conditions: The symptom is observed when a large number of interfaces are flapping.

  Workaround: Disable syslog traps. Use interface level link trap for capturing link up/down notifications.

- CSCsj87744

  Symptoms: Configuring a command with the string “do” inside a sub-mode may cause unexpected behavior.

  There is known issue that using the PVC names ending with “do” lead to refusing the command as not valid. The error message “% Invalid input detected at ’^’ marker.” will be displayed if the command is executed in sub-mode. If it is executed in ATM mode, there will be no error reported, but the pvc will be removed from configuration after reload.

  Conditions: The symptom is observed when using “do” as shorthand for “domain,” for example in **ipe domain** CLI.

Workaround: Do not use “do” keyword as shorthand in commands inside a sub- mode.

Related to ATM PVC names: do not use PVC names ending with “do”.

Further Problem Description: Commands starting with “do” will be interpreted as exec commands.

- 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.

- CSCsk24854

  Symptoms: With bidirectional multicast traffic, a router that is running Cisco IOS Releases 12.2(33)SB, 12.2(31)SB3, 12.2(28)SB7, or later versions may stop forwarding all traffic, or even crash. Ping/ARP fails from adjacent routers as all packets are dropped.

  Conditions: This symptom occurs when any event that causes multicast adjacency to be removed (temporarily) from PXF, causing packets to be punted to RP. Some examples are:

  1. Remove/add static rendezvous point IP address.
  2. Issue the **clear ip mroute *** command.
  3. PIM DR change

  Workaround: There is no workaround.

- CSCsk44165

  Symptoms: Packets are punted when bidirectional multicast traffic is sent in an Multicast VPN (MVPN) network. As a result, the router may experience high CPU utilization and LDP and OSPF neighborships may go down.

  Conditions: The symptoms occur when single MVPNs are configured and where traffic is sent from a single MVPN customer. It mostly occurs with bidirectional traffic

  Workaround: As the behavior is inconsistent, no complete workaround is available.

- CSCsk64158

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCsl14450

  Symptoms: Under a high load of multicast traffic, a Cisco router may unexpectedly reload due to a CPU vector 300 or bus error.

  Conditions: This symptom has been observed only in environments where more than 10 tunnels have been configured on the same device using multicast over these tunnels.

  Workaround: There is no workaround.

- CSCsl42732

  Symptoms: When the **no ip portbundle** command is issued, the portbundle feature is removed unconditionally without checking if the portbundle is assigned to a session and is in use.

  Conditions: This symptom is observed when the **no ip portbundle** command is issued.

  Workaround: Before unconfiguring portbundle, check if it is assigned to a subscriber session. If it is assigned, display a message and do not unconfigure portbundle.

- CSCsl62963

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

  Conditions: Seen on a Cisco 7200 router.

  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

- CSCsm44353

  Symptoms: Platforms that are acting as LACs may experience a reload in rare occasions due to variables not being initialized under this rare circumstance.

  Conditions: This crash can only occur only if the device is configured to act as a LAC, initiating L2TP tunnels to LNS devices.

  Workaround: There is no workaround.

- 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:

1. rpm-xfh10-z135 - shut & remove interface Switch1.4073
2. rpm-xfh09-z134 - shut & remove interface Switch1.4073
3. rpm-xfp11-l172 - remove interface Switch1.3172
4. rpm-xfp13-z074 - remove interface Switch1.4074
5. rpm-xfp04-l171 - remove interface Switch1.3171

- CSCsm56940

  Symptoms: Traceback seen while doing Telnet with SSH enabled.

  Conditions: Occurs when SSH is enabled on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsm60321

  Symptoms: A router may reset due to a bus error when removing the legacy traffic shaping (traffic-shape rate XXX) from the interface with the presence of traffic.

  Conditions: Having both the legacy traffic-shaping (traffic-shape rate XXX) and MQC shaping (through policy-map) configured on the interface and trying to remove either of them will cause this issue to occur.

  Workaround: Avoid making changes to the traffic-shaping configured on the interface with traffic crossing the interface.

- CSCsm82911

  Symptoms: 1. Although a shaping policy is applied to VAccess sessions, the shaping function is not bounding traffic to a specific rate. 2. The **show interface** command for the ATM interface shows “class-based queueing” instead of “per-vc queueing”.

  Conditions: The symptoms are observed under the following conditions:

  - A Cisco 7301 router that is running Cisco IOS Release 12.2(31)SB13 acting as LNS for PPTP/L2TP and configured to get an AVpair for MQC on Virtual- access interfaces with shaping. The shut/no-shut on the ATM interface results in session shaping not working.
  - When a queueing policy is enabled on a session that is associated to ATM VC, or when a queueing policy is enabled on ATM VC directly. The **show interface** shows “class-based queueing”. Here, “class-based queueing” does not mean that the ATM interface ignores ATM VC queueing. It still runs ATM VC queueing. In fact, under all circumstances a Cisco 7200 series and a 7301 router run Per-VC queueing and on top of every VC, it runs class-based queueing if a queueing policy is enabled on the VC directly or via sessions. The “class-based queueing” in the output of “show interface” is just to display specific detail. (It may be expected that the display is either “per- vc queueing” or “per-vc class-based queueing”. Later releases in 12.2SR already show “per-vc queueing” for such configurations.)

  Workaround: Clear and re-establish all sessions.

- CSCsm87702

  Symptoms: A Cisco 10000 series router may run out of PXF-memory and end up in a state not being able to create new PPPoE sessions.

  Conditions: This symptom is seen during an aggressive churning test with lawful intercept enabled on all sessions via Radius.

  Workaround: There is no workaround.

Further Problem Description: This may show up on live systems just very slowly, depending on LI-activity. The leak can be monitored by following the output of the **sh pxf cpu cef mem | i Mac|write|^Type|^C10** command.

- CSCso33199

  Symptoms: The router may exhibit the following symptoms when classification based on FR-DE and IP TOS is turned on:

  1. Packets with both FR-DE and IP precendence marked may not get classified.
  2. Ingress classification may not work at all.
  3. All packets may get classified under class-default irrespective of their precendence states.
  4. FR-DE plus TOS classification may work, but other classes in an ingress policy may not.

  Conditions: These symptoms are seen in a Cisco 7300 or Cisco 10000 router that is running Cisco IOS Release 12.2(33)SB. The symptoms are not seen in a Cisco 7200 router.

  Workaround: Detach and reattach the policy-map to the interface.

- CSCso37882

  Symptoms: A Cisco 7304 router with NSE100 may punt all MPLS-to-IP traffic from PXF to RP when egress interface is a VRF GRE tunnel interface.

  Conditions: The issue affects Cisco IOS Releases 12.2(28)SB and 12.2(31)SB.

  Workaround: There is no workaround.

  Further Problem Description: The issue is not seen with Cisco IOS Release 12.2 (25)S.

- CSCso75736

  Symptoms: A router may show error messages when applying/using a policy-map on ATM, having **set cos** *cos* configured.

  Conditions: This symptom appears when the policy gets applied during PPPoE session establishment.

  Workaround: The command is not supported on ATM interfaces and correcting the configuration prevents the error-messages for new VCs. Any VCs previously used with it already fail to get the right policy applied. To correct this, remove the pvc-in-range and reapply it with the previous configuration.

  Further Problem Description: This defect just moves the error-message to a warning. The function itself will stay unsupported on ATM-interfaces. After correcting the configuration tracebacks left over which required the system to reload. No impact seen by the tracebacks.

- CSCso82551

  Symptoms: A router reloads.

  Conditions: This symptom happens when many PPPoEoA sessions are created over AutoVCs.

  Workaround: Increase the VeryBig buffer pool so that there are no more misses, creates and trims. For example, use the following statements:

  buffers verybig permanent 7000 buffers verybig max-free 7000

- CSCso90970

  Symptoms: The **no ip proxy-arp** command that is configured under ISG enabled interface is not working.

Conditions: This symptom is observed on the ethernet interface, where an **ip subscriber** command is configured. Same interface allows disabling IP Proxy ARP with the **no ip proxy-arp** command, but the command is ignored.

Workaround: There is no workaround.

- CSCsq05997

  Symptoms: The following error messages may appear in the log file multiple times:

  ```
  %ARP-3-ARPINT: ARP table accessed at interrupt level 1,
  -Traceback= 0x61013944 0x60B61F80 0x60B5A2A4 0x6019DDAC 0x600FA37C 0x600FCC6C Because
  the message is generated frequently, the log file may fill up too soon.
  ```

  Conditions: The symptom is observed because an IOS component is accessing the arp cache table in the interrupt context, which against the design of the IOS module. The error message indicates that the software is in danger of causing the router to crash.

  Workaround: There is no workaround.

- CSCsq06754

  Symptoms: A router crashes with QoS while doing OIR on PA-A3-OC3MM.

  Conditions: This symptom is observed when a router crashes with QoS while doing OIR on PA-A3-OC3MM with continuous traffic flow.

  Workaround: The crash is not seen in following cases:

  1. With continuos traffic flow, shutdown the interface before OIR and give “no shut” once OIR process is over.
  2. When reloading the router with continuos traffic flow.

- CSCsq09377

  Symptoms: The ESR-HH-1GE card on a Cisco 10000 router may crash with the following message:

  ```
  "%PXF_NICKEL-2-IB_ERR_SPR: IB Stuck Pause Request Error in slot X/Y"
  ```

  Conditions: The crash is seen on a Cisco 10000 platform that is running Cisco IOS Release 12.2(31)SBX. Previous Cisco IOS versions are potentially affected. Some known conditions that trigger this error are:

  1. Continuously flapping the interface using **shut** and **no shut** of the ESR-HH-1GE interface.
  2. Changing the MTU size (it is seen only on ATM based cards).
  3. Continuously setting and resetting the negotiation using the **negotiation auto** and **no negotiation auto** commands on ESR-HH-1GE interface.
  4. Most of the customer issues that trigger this error are not yet known.

  Workaround: There is no workaround.

  Further Problem Description: The “IB_ERR_SPR” indicates that the egress data path of the LC is stuck, and the only way to recover the path is to reset the LC. In most of the conditions explained above, the LC was only stuck for few seconds, and in those cases, the LC was unnecessarily reset. In this fix the IB_ERR_SPR handling is improved to avoid such LC resets.

- 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 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.

- CSCsq24332

  Symptoms: A router may crash after displaying errors similar to:

  ```
  %QOS-3-ATLEAST_ONE_FAILOVER_ERR: Fail-over of dynamic interface failed
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x61A9F260
  ```

  Conditions: The symptom is observed on a router that is running Cisco IOS Release 12.2(31)SB11.

  Workaround: There is no workaround.

- CSCsq44072

  Symptoms: ATM VC are not getting enough traffic through due to VC flow control when no burst value is configured for the VC.

  Conditions: The symptom is observed when no burst value is configured for the VC.

  Workaround: Configure a lower burst value.

- CSCsq49176

  Symptoms: Router bus error crash on invalid address:

  ```
  System returned to ROM by bus error at PC 0x608BB8A4, address 0xC6000E8E
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x608BB8A4
  -Traceback= 608BB8A4 608EE2F4 600132B8 605B2140 60A26C20 605B1C54 605B2FB4
  ```

  Conditions: Occurred on a Cisco 7200 running Cisco IOS Release 12.2(28)SB6.

  Workaround: There is no workaround.

- CSCsq57238

  Symptoms: An interface is congested. A QoS policy-map is applied to the interface such that one of the traffic-classes receives only infrequent packets. That traffic class is seen to have higher than expected latency. If steady traffic is sent through the same traffic class, then latency is as expected and bandwidth is seen to be shared between traffic classes as per their relative bandwidth guarantees.

  Conditions: The symptoms are observed on any interface, but is most obvious with low speed interfaces such as ATM PVCs with 256k or less bandwidth.

  Workaround: If the traffic class with the infrequent traffic in configured with **priority**, then latency will be minimized. For ATM on NPEG100 specifically, adding an extra traffic-class with a **priority** command will put the driver in low-latency mode which will reduce latency for the traffic class with infrequent traffic. The extra traffic class does not need to match any traffic.

- CSCsq75661

  Symptoms: An ATM interface that is configured with a large number of PVCs may exhibit PVC provisioning problems after repeated interface flaps. The VCC count on the ATM interface would increase by a random number once after each flap.

  Conditions: This symptom is observed on a dual PRE2 system that is running Cisco IOS Release .2(31)SB12 code and operating in SSO mode.

Workaround: Router reload or PRE cutover.

- CSCsq77282

  Symptoms: Creating a sub-interface may occasionally cause a traceback

  Conditions: This may happen when configuring an ATM or SONET sub-interface.

  Workaround: There is no workaround.

- CSCsq89329

  Symptoms: There is a leak in system resources (SHDB).

  Conditions: This symptom occurs when a large number of PPPoE sessions are churned.

  Workaround: There is no workaround.

- CSCsr05501

  Symptoms: The following error message is displayed on the router console during initialization:

  "% NBAR Error: hwidb could not found"

  Conditions: This symptom may happen when the configuration has QoS policy maps attached to user sessions.

  Workaround: There is no workaround.

  Further Problem Description: It s a benign diagnostic message which does not imply any problem on the router and can be ignored.

- CSCsr08994

  Symptoms: Traceback is seen while running FRF12.

  Conditions: The symptom is observed during post-router check. The issue is seen with PRE-2.

  Workaround: There is no workaround.

- CSCsr10542

  Symptoms: Spurious memory access or crash is seen with fall-over configuration.

  Conditions: The spurious memory access is seen when fall-over is configured under a peer-session template.

  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

- CSCsr40935

  Symptoms: Router crashes when service policy is applied while traffic is flowing.

  Conditions: Occurs on a Cisco 7200 after applying policy map on PVC with traffic.

  Workaround: Stop traffic before applying service policy map.

- CSCsr43440

  Symptoms: Packets marked with dscp af31 are incorrectly classified as dscp2.

  Conditions: This issue has been observed on a Cisco 7300 with NSE-100 that is running Cisco IOS Release 12.2(28)SB9. Also seen in a repro that is using Cisco IOS Releases 12.2(28)SB9, 12.2(28)SB12 and 12.2(33)SB1.

  The QoS configuration has 3 hierarchies.

  Workaround: There is no workaround.

- CSCsr43944

  Symptoms: In a Multicast NAT setup when the traffic is flowing, half of the packets may be dropped with reason given as “Multicast Adjacency Drop”.

  Conditions: This symptom is observed on Cisco 7304 NSE 100 platform where Multicast NAT is configured and PXF is enabled. Multicast NAT is not supported when PXF support is enabled so all the Multicast NAT traffic is being punted to RP. The punted Multicast packets are destined to be rate limited to 500pps when they pass through RP. In this case, instead of rate limiting to 500pps, exactly half of the packets were dropped with the reason given as “Multicast Adjacency Drop” and half of them processed correctly (reason: “Multicast Drop Recovery Punt”).

  Workaround: Disable PXF using “no ip pxf” in configure mode.

- CSCsr68497

  Symptoms: The router crash when the **default pppoe enable** command is entered.

  Conditions: Occurs with 4094 PPPoE sessions active. When the above command is used to disable PPPoE under Ethernet subinterface, the router crashes.

  Workaround: There is no workaround.

- CSCsr93441

  Symptoms: After deleting and configuring back some timeslots for an ESR-4OC3- CHSTM1 card, the PRE3 of a Cisco 10000 series router crashes for a TLB exception. The same issue happens three minutes later when the same steps are applied to the backup PRE.

  Conditions: This symptom is observed after an upgrade to PRE3 and Cisco IOS Release 12.2(33)SB.

  Workaround: There is no workaround.

- CSCsu08166

  Symptoms: On a 8e3ds3 line card with L2 transport VC, changing the mode from ADM to PLCP and then performing an SSO causes CDVT that is attached to the L2 Transport VC to reset the standby continuously. CDVT is not supported for L2 Transport VC.

  Conditions: This symptom is observed on a Cisco 10000 series router with an 8e3ds3 line card.

  Workaround: There is no workaround.

- CSCsu23940

  Symptoms: The error message “Must remove traffic-shape configuration first” is seen, and QoS policy is not getting attached.

Conditions: This symptom is seen when unable to attach a queueing policy-map ("bandwidth" configured) through Frame-relay (FR) map-class to a FR-DLCI interface with FRTS enabled.

Workaround: There is no workaround.

Further Problem Description: This has a major functional impact as the QoS- Policy is not getting attached.

- 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
  ```

- CSCsu32104

  Symptoms: A PRE-3 that is running Cisco IOS Release 12.2(31)SB code may encounter a Redzone overrun memory corruption crash.

  Conditions: Unknown at this time.

  Workaround: Turn off Auto IP SLA MPLS by entering the **auto ip sla mpls reset** command.

- CSCsu39864

  Symptoms: If the startup configuration includes a boot host TFTP command that calls for a file that contains something other than interfaces, the PRE (the primary or the standby) crashes, and the remote configuration file does not make it to the active configuration.

  Conditions: The symptom is observed when the startup configuration includes a boot host TFTP command that calls for a file that contains something other than interfaces. If the remote configuration file consists of only interfaces (no matter how many), everything works as expected. This problem is seen in both Cisco IOS Release 12.2(31)SB13 and Release 12.2(33)SB2.

  Workaround: Do not have this option configured.

  Further Problem Description: Stack degradation or a CPU hog message might also appear on the screen.

- CSCsu42078

  Symptoms: A router may crash due to bus error caused by an illegal access to a low memory address.

  Conditions: This happens when a service-policy is applied to an interface.

  Workaround: Remove "ip cef distributed" from the configuration.

- CSCsu44992

  Symptoms: VPDN redirect functionality does not work.

  Conditions: Basic functionality is broken. No special condition is required.

Workaround: There is no workaround.

- CSCsu45879

  Symptoms: Route-reflector may fail to send withdraw for some prefixes.

  Conditions: The symptom is observed when there are PE routers in the same update group. One PE sends a route refresh message to the RR and the other PE sends a withdraw message for multiple routes.

  Workaround: There is no workaround.

- CSCsu48898

  Symptoms: A Cisco 10000 series router may crash every several minutes.

  Conditions: The symptom is observed with a Cisco 10000 series router that is running Cisco IOS Release 12.2(31)SB13.

  Workaround: Use Cisco IOS Release 12.2(31)SB11.

- CSCsu87257

  Symptoms: Data-Link Switching (DLSw) connection may get stuck in PCONN_WT state when transitioning from two connections to a single connection if the peer closes with a FIN instead of RST. This will prevent the DLSw peers from communicating.

  Conditions: The symptom is observed with Cisco IOS Release 12.2(31)SB, and with a peer router capable of a single DLSw TCP connection that attempts to close one of the two connections with a FIN.

  Workaround: IP addresses of the DLSw peers can be arranged so that the higher IP address closes first. The IOS peer should initiate the close.

- CSCsu89831

  Symptoms: A Cisco 10008 router may fail to intercept packets for static subnets.

  Conditions: The symptom is observed on a Cisco 10008 router with a PRE-2/3 routing engine that is running Cisco IOS Release 12.2(31)SB.

  Workaround: There is no workaround.

  Further Problem Description: Packets are not intercepted because the lawful intercept security ACL does not get applied. This issue is not seen in Cisco IOS Release 12.2(33)SB and dynamic prefixes are intercepted correctly.

- CSCsu92903

  Symptoms: The VRRP state machine transitions into the “Master” state even if the interface is shut down.

  Conditions: The symptom is observed only when the interface is configured with “vrrp <group> timers learn”, which triggers the state machine to leave the INIT state.

  Workaround: As long as timer learning is not configured the problem will not occur. However, if timer learning is required, the command may be entered and the interface can then be configured with “no shut” and then “shut”. The VRRP state machine will now return to the correct “INIT” state.

- CSCsu94782

  Symptoms: A Cisco 7300 series router with an NSE-150 may hang with a %SYS-2- NOTQ error message while responding to traceroute messages.

  Conditions: The symptoms are observed with a Cisco 7300 series router with an NSE-150. The router must receive traceroute packets on a port-channel main interface.

  Workaround: There is no workaround.

- CSCsu97934

  Symptoms: NPE-G1 is crashing with “pppoe_sss_holdq_enqueue” as one of the last functions.

  Conditions: Unknown.

  Workaround: Entering the **deb pppoe error** command will stop the crashing.

- CSCsv01559

  Symptoms: DS3ATM police does not behave as expected when we change the mode of the DS3ATM card.

  Conditions: The symptom is observed when DS3ATM is in non-default mode, and the output service policy is at the main interface.

  Workaround: There is no workaround.

  Further Problem Description: When the card is in PLCP mode actual bandwidth should be 40700 but police is using 44200 since there is no change in the queue bandwidth after mode change.

- CSCsv04674

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

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

  Workaround: There is no workaround.

- CSCsv04752

  Symptoms: An LI tap remains “Operational” even after tap removal.

  Conditions: The symptom is observed on a Cisco 10008 router with PRE-2/3 that is running Cisco IOS Release 12.2(31)SB and Release 12.2(33)SB.

  Workaround: Reload of the router removes the stale tap.

- 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.

- CSCsv05899

  Symptoms: A Cisco 10000 series router with dual PRE3s or PRE4s may hang.

  Conditions: The PRE-A will first observe the following error:

  ```
  %FILESYS-5-CFLASH: Compact flash card removed from peer PRE (PRE slot B), slot0
  ```

The PRE-B console will repeatedly show the following errors:

```
%SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (0/0),process
= Flash Card Monitor.
%SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (0/0),process
= Standby service handler.
```

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.

- CSCsv27825

  Symptoms: Per-session QoS on virtual-access interfaces, is seen on a LNS that terminates PPPoE sessions.

  The shaper in the parent policy-map is not working. There is no backpressure, and the QoS in the child policy-map never starts.

  Conditions: The shaper has inconsistent behavior, may work for some sessions and not for others.

  Workaround: There is no workaround.

- CSCsv45649

  Symptoms: Packets are getting tapped into one MD when multiple MDs have been configured.

  Conditions: The symptom is observed when both tap entries are in the same ACL.

  Workaround: There is no workaround.

- CSCsv66827

  Symptoms: Clearing the SSH sessions from a VTY session may cause the router to crash.

  Conditions: The symptom is observed when a Cisco 7300 series router is configured for SSH and then an SSH session is connected. If the SSH session is cleared every two seconds using a script, the symptom is observed.

  Workaround: There is no workaround.

- CSCsv73388

  Symptoms: “Circuit-id-tag” and “remote-id-tag” attributes may be duplicated in packets sent to the RADIUS server.

  Conditions: The symptom is observed with Cisco IOS Release 12.2(31)SB13.

  Workaround: Use Cisco IOS Release 12.2(31)SB14.

- CSCsv78555

  Symptoms: A router may crash when doing an OIR of a PA-CC card with traffic passing through the interface in PA-CC.

  Conditions: The symptom is observed with a Cisco 7300 HA system. An OIR of a PA-CC card after switchover might cause this issue.

  Workaround: There is no workaround.

  Further Problem Description: This is due to a race condition between the IPC packet processing of PA-CC and an OIR of the PA-CC card.

- CSCsv79584

  Symptoms: 0.0.0.0 binding with a 0 minimum lease gets created and subsequently removed on the DHCP unnumbered relay.

  Conditions: This symptom is observed when DHCP client sends a DHCPINFORM with ciaddr set to its address, but giaddr is empty. Relay fills giaddr with its IP address and the server replies to giaddr. Since the DHCPACK is in response to DHCPINFOM, lease-time option is absent. Relay receives the DHCPACK and tries to process it normally leading to the route addition.

  Workaround: There is no workaround.

  Additional Information: This behavior can indirectly have a negative impact on the system by triggering other applications to be called because the routing table change is triggered by such DHCP request. Examining "debug ip routing" for 0.0.0.0/32 reveals 0.0.0.0/32 route flapping.

- CSCsv82676

  Symptoms: Line protocol of many interfaces in the 24che1t1 card may go down.

  Conditions: The symptom is observed when the line card is reset or coming up when the timeslots of any one of the channels are changed.

  Workaround: A further card reset will bring you out of the situation.

  Further Problem Description: Encapsulations can be any (HDLC/Frame relay).

- CSCsv87923

  Symptoms: A router may reload randomly following an upgrade to Cisco IOS Release 12.2(31)SB13.

  Conditions: The symptom is observed under normal use with the following routers: Cisco 7201, 7301 and 7206 (with NPE-300).

  Workaround: There is no workaround.

- CSCsv89255

  Symptoms: "MTU exceeded punt" occurs in an mVPN circuit when traffic is flowing.

  Conditions: the router should have more than 255 interfaces (seen via "show pxf interface".)

  Workaround: There is no workaround.

- CSCsv95474

  Symptoms: The PRE4 standby RP may get stuck in "in progress to standby hot" mode.

  Conditions: The symptom is observed after an RP switchover. The standby RP becomes stuck in an "in progress to standby hot" state until the RF client times out and the active RP resets the standby RP again.

  Workaround: There is no workaround.

- CSCsv99599

  Symptoms: In an ISG setup, the gigaword may be incremented randomly by 1 in each accounting update.

  Conditions: The symptom is observed with Cisco IOS Release 12.2(31)SB12a. The following radius output shows the issue:

  ```
  DEBUG: Packet dump:
          Acct-Output-Packets = 43118
          Acct-Input-Gigawords = 0
          Acct-Output-Gigawords = 83
  ```

```
       Acct-Input-Octets = 4265182
       Acct-Output-Octets = 41795579

DEBUG: Packet dump:
       Acct-Output-Packets = 43172
       Acct-Input-Gigawords = 0
       Acct-Output-Gigawords = 84
       Acct-Input-Octets = 4266910
       Acct-Output-Octets = 41795147
```

The output shows about 54 packets incremented by 1 gigaword (4 GB of data) within about a 15 minute timeframe.

Workaround: Get the radius server to detect the increment of 1 gigaword after 15 minutes and to discard the previous accounting records.

- 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.

- CSCsw27965

  Symptoms: When manipulating ATM VCs, some traceback or a crash may be observed.

  Conditions: The symptoms are observed when LAC and LNS are configured to send Tunnel-Start, Tunnel-Link-Start, Tunnel-Stop and Tunnel-Link-Stop accounting records.

  Workaround: There is no workaround.

- CSCsw43272

  Symptoms: The VPDN user does not take LNS-assigned IP addresses when using the DHCP pool.

  Conditions: The symptom is observed whenever the DHCP server is unavailable or when the DHCP pool is exhausted.

  Workaround: There is no workaround.

- CSCsw51210

  Symptoms: A Cisco 7304 NSE-100 router may crash while unconfiguring the MFR interface.

  Conditions: The symptom is observed with a Cisco 7304 router with an NSE-100 and when configuring the MFR interface.

  Workaround: Avoid configuring MFR with the Cisco 7304 platform.

- CSCsw74389

  Symptoms: Traffic may not pass through the PA-MC-8TE1+ port adapter.

  Conditions: The symptom is observed if the PA-MC-8TE1+ is a member of a multilink bundle or if it is configured with MPLS.

  Workaround: There is no workaround.

- CSCsw78396

  Symptoms: A router may crash when removing a three-level hierarchical policy.

  Conditions: The symptom is observed with a Cisco 7300 series router with an NSE-150.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(31)SB13

Cisco IOS Release 12.2(31)SB13 is a rebuild release for Cisco IOS Release 12.2(31)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB13 but may be open in previous Cisco IOS releases.

Basic System Services

- 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.

- 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.

- CSCek60566

  Symptoms: Type of Service (ToS) reflected in a L2TP header is not working in Cisco IOS interim Release 12.4(10.8)T2 after configuring the **ip tos reflect** command on L2TP.

  Conditions: This symptom has been observed with Cisco IOS interim Release 12.4 (10.8)T2.

  Workaround: There is no workaround.

- CSCek71379

  Symptoms: A TCB related crash may be seen.

  Conditions: There are no specific conditions.

  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.

- CSCin99689

  Symptoms: The command to do a warm upgrade results in a warm reboot.

  Conditions: This symptom occurs if a warm upgrade is executed. It will result in a warm reboot, provided the warm reboot is enabled. Ideally it should load the new image. In case the warm reboot is not configured, the system will return to the ROMMON with an error message.

  Workaround: There is no workaround.

- CSCsa73179

  Symptoms: Memory corruption, possibly leading to a crash or other undesired behavior, can occur when the **no default-information originate** command is entered in router RIP configuration mode.

  Conditions: This symptom occurs only if both the RIP routing protocol and the OSPF routing protocol are configured on a router.

  Workaround: There is no workaround.

- CSCsd23579

  Symptoms: On PPP links that do not support duplicate address detection (DAD), the interface up state can be signaled too early, for example before the interface is actually up. As a result, OSPFv3 neighbor relationship is not established.

  Conditions: Any interface that does not support DAD could signal link local up before the interface is up.

  Workaround: There is no workaround.

- CSCsd90876

  Symptoms: Memory corruption occurs when a "| include" is used with a CLI command. An already in-use block gets freed and causes this corruption.

  Conditions: This symptom can happen with any usage when a "| include" is used with a CLI command. It was found using a script for IPSec that resulted in "Crash on OIR of IPSec SLC module."

  Workaround: There is no work around. It is a programming defect.

  Further Problem Description: It is a rare corner case memory corruption when a block gets freed even when it is in use. It is caught by a script under stress testing conditions which results in such a rare condition.

  While using CLI and "| include" it is rare to get such a corruption. If it happens, it will lead to box reload.

- 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.

- 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.

- 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.

- CSCsh29217

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

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

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

- 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. A switch crashes. We have a script running that will continuously ssh-v2 into the 3560 then close the session normally. 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 crash.

  Conditions: This problem is platform independent, but it has been seen on Cisco Catalyst 3560, Cisco Catalyst 3750 and Cisco Catalyst 4948 series switches. The issue is specific to SSH version 2, and its seen only when the box is under brute force attack. This crash is not seen under normal conditions.

  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 the Cisco public website: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml

- CSCsi61723

  Symptoms: A router may crash spontaneously and display the following message:

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

  Conditions: The symptom is observed on a router that is running Cisco IOS Release 12.2SB. RIP packets that go through many features in this environment (such as, RIP -> IP -> MLP -> PPP -> L2TP -> IP -> QoS/HQF -> driver) may also cause the stack overflow.

  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.

- 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.

- CSCsj22472

  Symptoms: When an IXIA-simulated BGP neighbor is not up, BGP is forced to delete the ARP entry for the IXIA host for a while. During that period, the router has to send ARP, and traffic is lost for a while.

  Conditions: While observed with other protocols, this symptom was noticed with a typical BGP configuration in which the peers are nonexistent. This would cause the SYN to be retransmitted multiple times, and after some threshold, the ARP entry would be purged.

  The ARP entries gets flushed out when the TCP retransmission timer expires. This causes the CEF adjacency to be lost, and performance can drop for packets going to that destination until the ARP is resolved again. This problem is *not* specific to BGP and is applicable to anything that rides over TCP.

  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.

  Impacts: May impact traffic forwarding.

  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.

- CSCsj60578

  Symptoms: When the minimum number of links has joined a multilink bundle, Network Control Protocols (NCPs) such as IPCP fail to come up.

  Conditions: This symptom can occur if both peers are configured with the **ppp multilink links minimum mandatory** command.

  Workaround: Remove the **ppp multilink links minimum mandatory** command from the configuration.

- CSCsj88665

  Symptoms: A device with a PA-MC-2T3+ may reset because of a bus error if a channel group is removed while the **show interface** command is being used from another telnet session at the same time, and then the telnet session is cleared.

  The device may also display Spurious Memory Accesses.

  Conditions: These symptoms have been observed in the latest Cisco IOS 12.4T and 12.2S releases.

  Workaround: Do not remove a channel group while using the **show interface** command for that interface.

- CSCsk09651

  Symptoms: A router crashes when a service policy is being attached, detached, or modified across a virtual template in the presence of traffic.

  Conditions: This symptom is observed on a router that is configured with MLPPP over FR on channelized interfaces. The shaping is enabled at FR interface as well as in the service policy.

  Workaround: There is no workaround.

- CSCsk60912

  Symptoms: MPLS forwarding table is empty on standby RP.

  Conditions: This symptom is observed after ISSU loadversion, or simply when standby RP is reloaded.

  Workaround: There is no workaround.

- CSCsk68846

  Symptoms: Router Crashed when removing grandchild policy

  Conditions: Seen on a Cisco 7304 Router.

  Workaround: There is no workaround.

- CSCsk75147

  Symptoms: A cbs3120 switch may crash during license installation, while reloading the slave switch that is being installed with license.

  Conditions: This symptom is observed when:

  1. Installing up to 10 licenses in one file on Slave 4 in one vty session.
  2. Reloading Slave 4 while installing the license on another vty session.

  Workaround: There is no workaround.

  Further Problem Description: The issue is related to Inter-Process Communication (IPC). The crash is due to accessing an already freed port info. But the crash may be prevented by adding a check atcipc_notify_session_closure.

- CSCsk86196

  Symptoms: After an hw-module stop/start command sequence, the PPP over L2TPv3 sessions on that module may stop forwarding any traffic. The L2TPv3 control plane may be up and running but no data will be received over the L2 circuit.

  Conditions: The symptoms occur on a Cisco 7300 series or 10000 series router when a **hw-module slot** *name* **stop/start** command is issued.

  Workaround: Reboot the router.

- CSCsl12315

  Symptoms: A router may crash.

  Conditions: The symptom is observed under the following steps:

  1. The OC12ATM card is replaced with a 6OC3POS card and the **no card** *6/0* command is entered.
  2. The 6OC3POS card is replaced with the OC12ATM card and the **no card** *6/0* command is entered.
  3. The original ATM configuration is copied by entering the **copy startup-config running-config** command.

  Workaround: There is no workaround.

- CSCsl54880

  Symptoms:

  – Gigabit Ethernet SPA will accept the multicast frames even though it is not destined for it.

  – Enabling bridging on Cisco 7304 SPA will break IP routing.

  Conditions:

  – Send multicast traffic which is not destined to that SPA.

  – Enable bridging and routing on the same interface.

  Workaround:

  1. Enable routing and bridging on separate interfaces.
  2. Enable both routing and bridging on the onboard Gigabit interface.

Further Problem Description: Both the above mentioned problems are happening because of the TCAM table entry.

- CSCsl62626

  Symptoms: A Cisco 7304 router may experience high CPU utilization (90-99%) when a large number (such as 2000) FR-L2TPv3 circuits are configured on a POS interface facing the CE router.

  Conditions: A Cisco 7304 router that is configured with an NSE-100 and that is running Cisco IOS Release 12.2(33)SB.

  Workaround: No other workaround than to reduce the scale of the circuits configured.

  Further Problem Description: CPU utilization is proportional to number of FR- L2TPv3 circuits. So the issue occurs for any number of FR-L2TPv3 circuits, but rises gradually as the number of circuits increase.

- CSCsl75177

  Symptoms: It is observed that BGP updates can be delayed in MPLS VPN network by BGP Route-Reflector towards RR-clients resulting in slower convergence.

  Conditions: This symptom is observed when BGP updates are delayed in MPLS VPN network.

  Workaround: There is no workaround.

  Further Information: This is an enhancement to the current route refresh mechanism and update groups.

- CSCsl77067

  Symptoms: Cisco 10000 Series Routers try to bring a configuration from a TFTP server (boot host). It appears the configuration gets transferred, but actually it is not accepted.

  Conditions: This issue occurs when redundant PREs are configured and try to create a few hundred subinterfaces or ATM PVCs through a configuration file obtained from a TFTP server that is called by means of the **boot host tftp** command on the startup-config.

  Workaround: Apply the **copy tftp run** command when either active or standby gets UP.

  Further Problem Description: The following messages are seen in the console during the boot process:

  ```
  Redundant RPs - Simultaneous configs not allowed:locked from console
  ```

  and then:

  ```
  %SYS-5-CONFIG_I: Configured from tftp://(url of the config) by console
  ```

  But it is not true. The file never actually gets to the active configuration.

  Configuring RPR+ does not help. The same message is seen:

  ```
  Simultaneous configs not allowed:locked from console
  ```

- 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.

- CSCsl94263

  Symptoms: A Cisco 7500 series router may crash.

  Conditions: This symptom occurs when SSO is configured on the Cisco 7500 router and when we try to reconfigure an existing service policy.

Workaround: There is no workaround.

Further Problem Description: The router crashes when trying to reconfigure the service policy, which is already configured on the router. The crash is seen when we try to configure the **random-detect dscp-based** command.

- CSCsl97384

  Symptoms: Router reload is seen in the network with a traceback when the **show aaa user all** command is executed.

  Conditions: This symptom occurs when the command is executed with 2k or more sessions in progress.

  Workaround: Do not enter the **show aaa user all** command.

  Further Problem Description: This is more like a timing or race condition, which could occur with a large number of sessions.

  The **show** command outputs data from General DataBase which is typically a hash table for each session. However, it does not lock the table during the display for each session. When we have a large number of sessions, the output process may take more than one pass. Meantime if we clear the session, we free the memory associated with that session's General DB. Now, pointers the **show** command is using, point to a freed memory resulting in a reference to a bad pointer. The output process has to sleep (suspend) a moment, and the crash occurs.

- 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.**

- CSCsm13783

  Symptoms: MVPN PIM adjacency cannot be established over the MDT tunnel.

  Conditions: The very basic functionality of MVPN is not functioning, because of which no multicast traffic can flow between PE2 and PE1.

  Workaround: There is no workaround.

- CSCsm14833

  Symptoms: All incoming ISDN calls are rejected.

Conditions: This symptom occurs when a Cisco IOS router is:

- equipped with NPE-G2.
- configured for ISDN dial-in with multiple Dialer Profiles.

This is seen in devices (Cisco 7206VXRs) that are configured for ISDN PRI dial- in with Dialer Profiles for backup purposes.

The problem could be reproduced in the lab where ISDN BRI i.o. PRI line is in use:

- When only 1 Dialer Profile is configured, all incoming ISDN calls are bound to it by default.
- When 2 Dialer Profiles are configured in the same pool, all incoming ISDN calls were rejected due to “Incoming call rejected, unbindable”.

The Caller ID or DNIS binding cannot be used as all incoming ISDN calls have no Caller ID and the same DNIS.

Workaround: Upgrade to Cisco IOS Release 12.4(11)T or later releases, which also support NPE-G2.

- CSCsm16355

  Symptoms: A Cisco 10000 series router may reload unexpectedly during aggressive ISG PPPoA call bringup.

  Conditions: The symptom is observed in system test on a Cisco 10000 series router that is running Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCsm17596

  Symptoms: In PRE2, the throughput of traffic sent in a given QOS class can flap.

  Conditions: The symptom is seen when a class is overloaded with CIR=0.

  Workaround: Use a policy-map with bandwidth instead of bandwidth remaining. This will set a CIR other than zero for those classes.

- CSCsm43181

  Symptoms: VPNv4 routes are not deleted from the VRF RIB when withdrawing VPNv4 BGP routes. This results in routes being present in VRF RIB, although the routes are not in the VPNv4 BGP table.

  Conditions: This symptom happens when SSO is enabled.

  Workaround: Remove SSO configuration from all BGP peers to avoid the problem. If the problem happens, use the **clear ip route vrf vrf-name prefix** command to clean up the related entry in RIB.

- CSCsm61105

  Symptoms: The router can crash due to bus error. The crash is seen after repeatedly after removing virtual-template interfaces under ATM.

  Conditions: The crash is seen under the following conditions:

  1. Bring up nearly 3000 PPPoE and PPPoEoA sessions.
  2. Configure **no interface virtual-template** *number* under ATM interfaces

  Repeating Step 2 continuously will cause a crash.

  Workaround: There is no workaround.

- CSCsm73602

  Symptoms: High CPU load due to VTEMPLATE Backgr process.

Conditions: This symptom occurs when **ip multicast boundary** command is used on many interfaces (8000 or more).

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.

- CSCsm93411

  Symptoms: A Cisco 10000 series router may display the following message when altering MTU size on the ATM interface:

```
%C10KEVENTMGR-1-IRONBUS_FAULT: IB Stuck Pause Request Error 3/1, Restarting
Ironbus
   %C10KEVENTMGR-1-IRONBUS_SUCCESS: IB Stuck Pause Request Error 3/1, Restart
Successful
```

  Conditions: This symptom may occur when changing MTU value on ATM interface and one of its subinterfaces. The error message is seen with the OC-3 ATM line card.

  Workaround: There is no workaround.

- CSCso09458

  Symptoms: SPAs in an MSC-100 may go missing.

  Conditions: The symptom is observed when you have entered the **hw- module slot slot_num stop** command, then do a switchover and then enter the **hw-module slot slot_num start** command in a new active.

  Workaround: Enter the command **hw-module subslot slot_num reload**.

- CSCso10458

  Symptoms: Standby reloads due to RF timer expiry during SNMP platform sync.

  Conditions: This symptom occurs when the system is coming up in stateful switchover (SSO) mode.

  Workaround: There is no workaround.

- CSCso18630

  Symptoms: SNMP counters on the 64-bit counters for incoming traffic, ifHCInOctets, are reporting very high values, different from what CLI reports, and even greater than the physical interfaces capacity.

  Conditions: This symptom may be seen with all line cards (PA-CC, SPA, LCs) on a Cisco 7300 router with NSE-100 that is running c7300-p-mz.122-31.SB10.bin.

  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.

- CSCso25666

  Symptoms: On the CH-OC12 and CH-OC3 line cards, when issuing a controller **no framing** command while MR-APS is configured on the controller, the line card may reload.

  Conditions: This symptom is observed on a Cisco 10000 series router.

  Workaround: Remove MR-APS configs on controller before removing the framing (no framing).

- CSCso35153

  Symptoms: When a large scale configuration of PPPoXoA sessions is used with ATM range PVCs using create-on-demand, it is possible to have a large quantity of tracebacks occur along with a 100% CPU utilization spike. During this event, sessions will not be able to connect or reconnect, and VTY connections will not respond. This occurs when some or all of the sessions are brought down.

  Conditions: This symptom is seen with an environment of 8000 PPPoEoA sessions across 8000 create-on-demand range PVCs following the issuing of the **clear pppoe all** command.

  Workaround: Do not bring down sessions in large quantities.

- CSCso38361

  Symptoms: A multicast S,G entry is deleted and rebuilt every 3 minutes and 30 seconds. Additionally, the T bit is not set. Depending on the network topology and RP placement, this can break end to end multicast connectivity.

  Conditions: This issue is seen on a Cisco 7304 NSE-100 with PXF enabled and is running Cisco IOS Release 12.2(31)SB5 or Release 12.2(31)SB11.

  Workaround: Disable PXF or remove **ip vrf select source** from the source facing interface.

- CSCso39444

  Symptoms: SP/LC might crash after SSO cutover.

  Conditions: This problem is a timing issue and would be more easily seen in SSO cutover case.

  Workaround: There is no workaround.

- CSCso45720

  Symptoms: When a vendor client is l2-connected to an ISG interface, and the client does DHCP, the client will perform a DAD ARP after it receives the offer.

  In the ARP, it uses 0.0.0.0 in the “sender-ip-address” field, in which the ISG will respond. This causes the client to assume this IP already exists on the network, and it sends back a DHCP decline to the DHCP server. Aside from the client failing to get an IP address, this issue can also deplete the IP pool.

  Conditions: This symptom happens with some third-party vendor clients.

  Workaround: If we get ARP REQ with source address 0.0.0.0, we would send IP_ARP_ACCEPT directly and let ARP handle this situation. Basically ISG does not want to influence in that case, so the relevant code changes.

- CSCso47048

  Symptoms: A router may crash with the following error message:

  ```
  %SYS-2-CHUNKBADFREEMAGIC: Bad free magic number in chunk header, chunk 6DF6E48
  data 6DF7B48 chunk_freemagic EF430000 -Process= "Check heaps", ipl= 0, pid= 5,


  -Traceback= 0x140C170 0x1E878 0x1EA24 0x1B4AC 0x717DB8
  chunk_diagnose, code = 2
  ```

```
chunk name is PPTP: pptp_swi

current chunk header = 0x06DF7B38
data check, ptr = 0x06DF7B48

next chunk header = 0x06DF7B70
data check, ptr = 0x06DF7B80

previous chunk header = 0x06DF7B00
data check, ptr = 0x06DF7B10
```

Conditions: This issue has been seen on Cisco 7200 router with NPE-G2 configured for L2TP and running Cisco IOS Release 12.4(15)T3 and Cisco IOS Release 12.4(15)T4.

Workaround: There is no workaround.

- CSCso50635

  Symptoms: Local switching connection will not pass traffic after using the **hw-module reset** command.

  Conditions: This symptom occurs while doing **hw-module reset** *slot*, where local switching connection is configured with at least one segment as ATM PVC on *slot*.

  Workaround: Micro code reload will bring the system back.

- CSCso59866

  Symptoms: A Cisco 10000 series router may crash when configured for Authentication, Authorization, and Accounting (AAA).

  Conditions: No special conditions are known for causing this crash.

  Workaround: There is no workaround.

  Further Problem Description: The issue was reported for a customer specific special based on Cisco IOS Release 12.2(31)SB9.

- CSCso64405

  Symptoms: A Cisco 10000 router sends out ARP and PPPoE active discovery control packets with CoS bits as 6 in 802.1Q header (these bits are also referred as Priority Bits) Cisco IOS Release 12.2(31)SB. This has been a behavior difference from earlier releases, which can bring out issues in network if such packets are treated differently.

  For example, a network which is configured to drop packets with CoS value 6 would see behavior difference.

  Conditions: This is a default condition.

  Workaround: Configure network to allow packets with different CoS values. Note that this is applicable only if the network is configured to drop such packets.

- CSCso66459

  Symptoms: ToS is always 0x00 when exporting the Netflow information to the Netflow collector. In the output of the **sh ip cache verbose flow** command, the ToS value is correct.

  Conditions: This symptom is observed on a router that is running with PXF and using Netflow Export version 5.

  Workaround: Disable PXF with the **no ip pxf** command.

- 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** *number* under ATM interfaces.

  Repeating Step 2 continuously will cause a crash.

  Workaround: There is no workaround.

- CSCso75868

  Symptoms: Some ATM subinterfaces stop the output of the packets after SSO. After **shut/no shut** on the defective subinterface, it comes to output the packets.

  Conditions: Though the Encap String is displayed on the normal subinterfaces by the **show ip cef** *VRF IP* **plat** command, no Encap String is displayed on the defective subinterface after the SSO by the **show** command.

  Encap String:

  After **shut/no shut** on the defective subinterface, Encap String comes to be displayed on it by the **show** command.

  ```
  Encap String: 0408000000000000AAAA030000000800
  ```

  Workaround: There is no workaround.

- CSCso76044

  Symptoms: Whenever a subinterface is created on ESR-6OC3/P-SMI with Cisco IOS c10k2-k91p11-mz.122-31.SB9a, it sends an error. It works fine with Cisco IOS Release 12.2(27)SBB4c.

  Conditions: Unknown.

  Workaround: There is no workaround.

- CSCso84507

  Symptoms: When a downgrade is done from Cisco IOS Release 12.2(33)SB to Release 12.2(31)SB, the Standby that is loaded with Cisco IOS Release 12.2(31)SB fails to do config sync and keeps crashing.

  Conditions: This symptom occurs when both Active and Standby are loaded with Cisco IOS Release 12.2(33)SB image with PPPOX (PPPoA or PPPoE) configurations. Standby is downgraded to Cisco IOS Release 12.2(31)SB. The standby loaded with Cisco IOS Release 12.2(31)SB fails to do configuration sync and keeps crashing after configuring **issu loadversion** command.

  This is also seen in the case of an upgrade from Cisco IOS Release 12.2(31)SB* to Cisco IOS Release 12.2(33)SB image, after **issu runversion** command, when Active has Cisco IOS Release 12.2(33)SB and Standby has Cisco IOS Release 12.2(31)SB* image.

  Workaround: For upgrade from Cisco IOS Release 12.2(31)SB* to Cisco IOS Release 12.2(33)SB image:

  After **issu runversion** command, when Active has Cisco IOS Release 12.2(33)SB:

  1. Configure the following:

     ```
     router#configure terminal
           router(config)#redundancy
           router(config-red)#force-rpr 1
     ```

2. Cisco IOS Release 12.2(31)SB* becomes Standby and will crash once and then come up in RPR mode.
3. Do **issu commitversion** and Standby will come up with Cisco IOS Release 12.2(33)SB image.

For downgrade from Cisco IOS Release 12.2(33)SB to Cisco IOS Release 12.2(31) SB* image:

1. Configure the following on Active PRE Cisco IOS Release 12.2(33)SB:

```
router#configure terminal
      router(config)#redundancy
      router(config-red)#force-rpr 1
```

2. Do **issu loadversion** command, which causes Standby to go down and come up as Standby (Cisco IOS Release 12.2(31)SB*). The new Standby will crash once and then come up in RPR mode.
3. Do **issu runversion** command to make Standby as Active (Cisco IOS Release 12.2(31)SB*).
4. Do **issu commitversion** command and Standby will come up in Cisco IOS Release 12.2(31)SB*.

The **force-rpr 1** command is removed from the configuration by now, since Cisco IOS Release 12.2(31)SB* image does not support this command.

- CSCso85386

  Symptoms: A Cisco PRE-2 that is running Cisco IOS Release c10k2-k91p11-mz.122- 27.SBB4c image crashes and fails after customer removes an interface and ran some **show** commands.

  Conditions: This symptom is observed on a Cisco 10000 series PRE-2.

  Workaround: There is no workaround.

- CSCso88718

  Symptoms: Sessions come up on LNS even after the associated VT on the LAC has been removed.

  Conditions: This symptom is seen when the BBA group should have virtual- template configured in it even after deleting the virtual-template interface.

  Workaround: Remove virtual-template configuration from the BBA group.

- CSCsq11427

  Symptoms: There may be a small amount of memory leak for each PPP connection.

  Conditions: The symptom is observed when PPP authorization is in use and the PTA session flaps. This problem will be seen only when the **ip address pool** or **ip address** commands are assigned from the radius-server.

  Workaround: There is no workaround.

  Further Problem Description: PPP attempted to set authorization information into IPAM for each connection. But the attempt by IPAM to store that information in the PPP Author sub-block off the PPP context failed because of the failed registration. The error exit for this failure did not clean up the IPA block just created and caused the memory to leak. This leak occurred on every PPP connection.

- CSCsq15983

  Symptoms: When an interface is **shut**, the LC reloads and PRE switches over. On the new active when the interface is **no shut**, the VCs do not come up.

  Conditions: This symptom is observed on the Cisco 10000 series router.

Workaround: If PVC is in DOWN state, do a **shut** followed by a **no shut** to recover. If PVC is in INACT state, resetting the LC is required to recover.

- CSCsq18413

  Symptoms: For iEdge policies on the Cisco 10000 series router, if the TCAM entries get full, there will be a perpetual high CPU of greater then 90%, with SuperACL accounting for most of the CPU use.

  Conditions: The risk of hitting this condition increases for specific combinations of iEdge traffic classes, where there are many overlapping ACE entries across the traffic classes.

  Workaround: Avoid having overlapping ACEs across traffic classes that are part of the iEdge policy.

- CSCsq19159

  Symptoms: System crash or memory corruption occurs.

  Conditions: Occurs when repeated line card resets are seen in the device or repeated line card online insertion and removal (OIR) operations are performed.

  Workaround: There is no workaround.

- CSCsq19874

  Symptoms: Standby reloads following cutover.

  Conditions: This symptom occurs during an upgrade to Cisco IOS Release 12.2(33) SB on Cisco 10000 series router with RPR+ configured redundancy mode. This results in RPR fallback mode being employed (correctly) and with PRE-B as the active, running the earlier release.

  Workaround: Perform the upgrade procedure with PRE-A as the active and PRE-B as standby.

- CSCsq28480

  Symptoms: The following message is printed on the console:

  ```
  Policy-map installation via subscriber-profile not supported
  ```

  Conditions: This symptom occurs when an unsupported policy-map is downloaded via the subscriber profile.

  Workaround: There is no workaround other than not using unsupported policy maps.

  Further Problem Description: If this happens to 32,000 sessions, then 32,000 messages will be printed on the console at 9,600 baud.

- CSCsq28584

  Symptoms: A router may crash from memory corruption.

  Conditions: The symptom is observed when a QOS policy is added to the service template in the BroadHop. It may also be observed if service with TC and L4Redirect action is installed on a subscriber profile.

  Workaround: There is no workaround.

- CSCsq30252

  Symptoms: An E1 controller may flap due to RMAI alarms, even after an internal loop in ESR (with internal clocking) is added.

  Conditions: The symptom is observed on an ESR that is running Cisco IOS Release 12.2(31)SB.

  Workaround: Use the **temux force workaround ds1e1 x y** command.

  Further Problem Description: This issue appears to be corner case.

- CSCsq31206

  Symptoms: A router that is running in SSO mode can crash when PPPoX sessions are being brought up with the following messages appearing in crashinfo file and on router console:

  ```
  %SYS-3-OVERRUN: Block overrun at 7A3280D8 (red zone 00000000)
  %SYS-6-BLKINFO: Corrupted redzone blk 7A3280D8, words 2348, alloc 605CAEC8,
  InUse, dealloc 0, rfcnt 1
  ```

  Conditions: This symptom occurs when a router that is running in SSO mode may crash when PPPoX sessions are being brought up. The crash does not occur when local authentication method is used.

  Workaround: There is no workaround.

- CSCsq31602

  Symptoms: DBS enabled VCs are not syncing to standby RP. This issue is reproducible even with a single VC when the router is reloaded.

  Conditions: This symptom is observed on a Cisco 10000 series router that is a HA setup with SSO mode configured.

  Workaround: Resetting the standby will bring the VCs up.

  Further Problem Description: This will effect the synchronization of PPP sessions to standby.

- 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 points to drop entry.

    ```
    router#<CmdBold>show mpls forward vrf <vrf name> x.x.x.x<noCmdBold>
     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#<CmdBold>show ip cef vrf <vrf name> x.x.x.x int<noCmdBold>
[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: The eiBGP multipath is enabled; iBGP path comes up first, then the eBGP path. Both eBGP and iBGP paths could be in MPLS forwarding causing the issue.

Workaround: Using the **clear ip route vrf** *name* **x.x.x.x** clears the issue.

- CSCsq32027

  Symptoms: A crash may occur when a PPPoX session with an active Lawful Intercept (LI) tap is disconnected.

  Conditions: This symptom is observed when SNMP LI tap is applied to a PPPoX session. Session disconnect is required.

  Workaround: There is no workaround.

- CSCsq38077

  Symptoms: For a DS3E3 ATM line card, if the line card is reset with any one of the 8 ports shut, the card comes up fine and all the VCs in the UP port work fine.

  On **no shut** of the previously shut port:

  – The VC under this port comes up and forwards traffic, but all the VCs under other ports fail to forward traffic.

  – May report an Ironbus restart sometimes after issuing **no shutdown** on ATM port.

  Conditions: This symptom is observed only in DS3 ATM line card.

  Workaround: Reset the card again to recover the failed VCs.

- CSCsq41463

  Symptoms: A Cisco 10000 series router with POS card with redundant PREs is running Cisco IOS Release 12.2(31)SB2 in RPR+ mode. The POS interface is using PPP encapsulation. When the Cisco IOS is upgraded from Cisco IOS Release 12.2(31)SB2 to Release 12.2(31)SB10, the POS interface does not come up after redundancy failover.

```
Router>en
Router#sh ip int brie
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0/0      unassigned      YES NVRAM  up                    down
POS5/0/0               10.10.10.2         YES NVRAM  down                  down
```

  Conditions: This symptom is seen when the Cisco IOS is upgraded to Cisco IOS Release 12.2(31)SB210 and Release 12.2(31)SB11 using the following procedure:

  1. Put new Cisco IOS Release 12.2(31)SB10 image on both PREs in flash cards.
  2. Modify the **boot** commands to make router boot from new images.
  3. Reset standby PRE which then boots from new Cisco IOS Release 12.2(31)SB10.

4. Perform switchover which causes Primary PRE to reset and boot from new Cisco IOS Release 12.2(31)SB10.
5. Both PREs are up with new Cisco IOS with slot B PRE as Active and Slot A PRW as Standby Warm.

Workaround: A **shut/no shut** on the POS interface will bring up the POS interface with PPP encapsulation.

```
Router#sh ip int brie
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0/0      unassigned      YES NVRAM  up                    down
POS5/0/0               10.10.10.2         YES NVRAM  down                  down
Router#
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int pos5/0/0
Router(config-if)#shut
Router(config-if)#
00:06:36: %C10K_ALARM-6-INFO: CLEAR CRITICAL POS 5/0/0 Physical Port Link Down
00:06:36: %C10K_ALARM-6-INFO: ASSERT INFO POS 5/0/0 Physical Port Administrative
State Down
00:06:36: %LINK-5-CHANGED: Interface POS5/0/0, changed state to administratively down
Router(config-if)#no shut
Router(config-if)#
00:06:44: %C10K_ALARM-6-INFO: CLEAR INFO POS 5/0/0 Physical Port Administrative State
Down
00:06:44: %LINK-3-UPDOWN: Interface POS5/0/0, changed state to up
00:06:44: %C10K_ALARM-6-INFO: ASSERT CRITICAL POS 5/0/0 Line Remote Failure
Indication
00:06:44: %SONET-4-ALARM:  POS5/0/0: LRDI
00:06:59: %C10K_ALARM-6-INFO: CLEAR CRITICAL POS 5/0/0 Line Remote Failure Indication
00:07:01: %LINEPROTO-5-UPDOWN: Line protocol on Interface POS5/0/0, changed state to
up
Router(config-if)#^Z
Router#
Router#sh ip int brie
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0/0      unassigned      YES NVRAM  up                    down
POS5/0/0               10.10.10.2         YES NVRAM  up                    up
Router#
```

- CSCsq49238

  Symptoms: A router crashes while removing the policy in the c10k_iedgre_extract_tc function.

  Conditions: There should be around 24k sessions with extremely low memory at the box, and sessions should be flapping (coming and going). There should also be traffic class applied to the session.

  Workaround: There is no workaround.

- CSCsq49852

  Symptoms: Memory is used and held by the EXEC process or found in *Dead*.

Conditions: The symptom is observed when the **show sss session detailed** command is used, and the ISG policy map is configured with "subscriber condition-map match-any internet-service."

Workaround: There is no workaround.

- CSCsq51300

  Symptoms: Stats for a few ACL templates are not updated correctly.

  Conditions: This symptom occurs when there is a large number of ACLs (4096). Send traffic across and check the stats on all of them.

  Workaround: There is no workaround.

- CSCsq52267

  Symptoms: For certain iEdge traffic class configurations, the SuperACL process may consume hundreds of megabytes of memory. While it releases this memory, the sudden spike in memory consumption (for example, when an iEdge policy is compiled due to a new incoming session) has the potential to create other system failures.

  Conditions: The symptoms can be triggered if there are four or more traffic classes in an iEdge policy, and there are several duplicate ACEs across these traffic classes. The issue is amplified with the number of iEdge traffic classes.

  Workaround: Optimize the traffic class configurations. For example, remove the duplicate ACEs that may be present across several traffic classes.

- CSCsq53018

  Symptoms: The LSP ping is not working over GRE tunnel.

  Conditions: This symptom occurs with PXF enabled.

  Workaround: There is no workaround.

- CSCsq63624

  Symptoms: The bandwidth of the police percent is not updating properly for Multilink PPP over ATM (MLPoATM), LFI over ATM (LFIoATM), LFI over Frame Relay (LFIoFR) and single member MLP on LNS, when attaching the policy map to the Multilink interface.

  Conditions: The symptoms are observed when bringing up the MLPoATM, LFIoATM, LFIoFR and single member MLP on LNS with a single link and attaching the police percent on the Multilink interface.

  Workaround: Use police absolute value instead of police percent.

- CSCsq69755

  Symptoms: The following error messages may start showing up in syslog:

  ```
  %IDBINDEX_SYNC-3-IDBINDEX_ENTRY_ADD: Cannot add entry to interface index
  table: "", 21

  %COMMON_FIB-2-IF_NUMBER_ILLEGAL: Attempt to create CEF interface for Virtual-
  Access2.2631 with illegal if_number: -1
  ```

  Conditions: This occurs after the box has gone through some sessions churning and switchovers.

  Workaround: There is no workaround.

  Further Problem Description: If these messages appear in syslog continuously, schedule a reboot before it crashes.

- CSCsq75350

  Symptoms: Flow accounting records (start/stop/interim) may not be generated for PPP sessions.

  Conditions: The symptom is observed when Traffic-Class based service is applied to a PPP session using on-box configuration or service log-on.

  Workaround: There is no workaround.

- CSCsq78381

  Symptoms: Port adapter carrier card loss of heartbeat occurs as seen in the following display:

  ```
  %PACC-3-HEARTBEAT_LOSS: PA Carrier Card Loss of heartbeat
  ```

  Conditions: This symptom happens when a router boots up with all the PAs up.

  Workaround: There is no workaround.

- CSCsq78734

  Symptoms: If the service-policy is attached on the main interface and packets are routed through the sub interface, the packets are not egressed out. Also PACC-3-HEART_LOSS is seen on the port-adapters.

  Conditions: This issue is seen with Cisco 7300(NSE-100) router with PXF enabled.

  Workaround: Disable PXF using the **no ip pxf** command.

- CSCsq88522

  Symptoms: Convergence time is greater than expected in high availability SSO mode.

  Conditions: This issue occurs only when the **no aaa new- model** command is enabled for high available sessions such as PPPoSerial that do not need external AAA server support. This issue is observed with more than 2000 serial interfaces.

  Workaround: There is no workaround.

- CSCsq91788

  Symptoms: A Cisco 10000 series router crashes on loading negative configurations.

  Conditions: This symptom happens when loading provisioning/unprovisioning LS and/or PW connection scale configurations from TFTP while executing the **show xconnect all detail** command on other console.

  Workaround: There is no workaround.

- 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.

- CSCsq93407

  Symptoms: On a Cisco 10000 series router, after some hours of normal operation, both input and output traffic accounting stops increasing for volume monitor prepaid services associated with a random ISG session.

Conditions: The symptom is observed with ISG sessions with volume monitor prepaid service only and this is been seen when the drop is set while doing a reauthorization. The issue is seen only when the policy is been shared by multiple ISG sessions.

Workaround: Configure an explicit event to set a drop to FALSE in the control policy at quota depletion/exhaustion.

- CSCsq93887

  Symptoms: A router may crash while trying to execute the **show interface serial** command on a 4CHSTM1 card.

  Conditions: The symptom is observed when a channel is removed and the corresponding **show interface serial** command is executed simultaneously from the other VTY.

  Workaround: Execute the **show interface serial** command only after the channel is removed.

- CSCsr04131

  Symptoms: Standby continuously reboots after switchover.

  Conditions: This symptom occurs on an optimally loaded router (router with some 300k routes) when switchover is performed after change in configuration without performing a reload.

  Workaround: Perform reload on the router before performing switchover whenever there is any major configuration changes on the router.

- CSCsr13399

  Symptoms: Topology:

  Router PPPoE/PPPoA <----> 7301.

  The PPP session is established with the Cisco 7301, which is ISG enabled.

  When traffic reaches 1 gigabyte, the accounting attribute will be corrupted with 2^32 - 1.

  The expectation of the gigabyte word is when it reaches 4294967295 bytes, it will increment with 1 gigaword.

  The problem is seen in the following releases:

  Cisco IOS Release 12.2(31)SB11: per-user service account corrupts the gigaword, and per-user session is correct.

  Cisco IOS Release 12.2(31)SB12: per-user service account corrupts the gigaword, and per-user session does not show anything at all.

  Cisco IOS Release 12.2(33.1.10)SB1: per-user service account shows nothing in the gigaword, and per-user session is correct.

  Conditions: When traffic reaches 1 gigabyte, the accounting attribute will be corrupted with 2^32 - 1.

  Workaround: There is no workaround.

- CSCsr19860

  Symptoms: The standby may reload when upgrading the software from Cisco IOS Release 12.2(31)SB to Cisco IOS Release 12.2(33)SB1.

  Conditions: This symptom occurs at run version during client verification.

  Workaround: There is no workaround.

- CSCsr41244

  Symptoms: The standby PRE may reset after adding an ISG service policy to a Virtual-Template, followed by the **clear pppoe all** command. New sessions start coming up.

Conditions: This problem may occur after adding an ISG service policy to a Virtual-Template, followed by the **clear pppoe all** command. New sessions start coming up.

Workaround: There is no workaround.

- CSCsr53027

  Symptoms: A router crashes after a couple of switchovers in the Cisco 10000 iEdge area.

  Conditions: This symptom is observed when ISG policies are configured at the router. A couple of switchovers must be done.

  Workaround: There is no workaround.

  Further Problem Description: This problem occurs due to the virtual access numbers (if_number) equal to -1.

- CSCsr57376

  Symptoms: A router crashes due to a TLB exception.

  Conditions: This symptom is seen while deleting the class-default class map in a MQC policy map that is applied to thousands of PPPoX sessions.

  Workaround: There is no workaround.

- CSCsr65585

  Symptoms: Features intermittently fail to be installed for users.

  Conditions: This symptom occurs under the following conditions:

  - Running ISG
  - Having 1000s of DHCP initiated subscribers using the iEdge features, for example L4R, PBHK, etc.
  - Applicable to Cisco 10000 series router only

  Workaround: Reload, or if possible switchover to other PRE.

- CSCsr68082

  Symptoms: A router crashes when unconfiguring multipoint ATM subinterface that is configured to bring up PPPoA sessions.

  Conditions: This symptom is seen when unconfiguring multipoint ATM subinterface that is configured to bring up PPPoA.

  Workaround: There is no workaround.

- CSCsr73116

  Symptoms: A Cisco 10000 series router (PRE3) crashes on active and standby PRE3 with the following error:

  ```
  PRE3 crash: COB3_FCPU_LQ_OFF_ERR: Low Priority Offset Error
  ```

  Conditions: This symptom is observed on a Cisco 10000 series router that is running Cisco IOS Release 12.2(31)SB10.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(31)SB12

Cisco IOS Release 12.2(31)SB12 is a rebuild release for Cisco IOS Release 12.2(31)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB12 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCec34459

  Symptoms: A memory leak may occur in the "IP Input" process on a Cisco platform, and memory allocation failures (MALLOCFAIL) may be reported in the processor pool.

  Conditions: This symptom is observed on a Cisco platform that is configured for Network Address Translation (NAT).

  Workaround: There is no workaround.

- 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.

- 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.

- CSCek59453

  Symptoms: A spurious memory access may be generated on a router.

  Conditions: This symptom is observed on a Cisco router when you configure an ATM VC on which PPPoE sessions are established. The trigger is when the VC is torn down.

  Workaround: There is no workaround.

- CSCek71844

  Symptoms: When the **virtual-profile** command is configured, PPP sessions do not come up.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCek77555

  Symptoms: PPP may not start on a serial interface that is physically up. When this situation occurs, inspection of the interface via the **show interface** command shows that the physical layer is up, but that the line protocol is down, and that LCP is closed.

  Conditions: This symptom is observed only on regular serial interfaces that use PPP encapsulation. The symptom does not occur with tunneling mechanisms such as PPP over ATM (PPPoATM) or VPDN sessions. The symptom may occur when the physical layer undergoes multiple state transitions, starting from an up state and ending in an up state, with the entire sequence occurring over a short period of time. In such a situation, event filtering mechanisms in Cisco IOS software may prevent a notification from being sent to PPP when the link returns to an up state, and, in turn, PPP from (re-)starting on the interface. The most likely time for such a situation to occur is when PPP itself resets the interface, which occurs when an existing PPP session is terminated because of a keepalive failure or LCP negotiation failure.

  Workaround: Any sequence that resets the physical layer and that is slow enough that the filtering mechanisms do not once again intrude is sufficient to restart PPP. For example, you can restart PPP on the interface by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCek78237

  Symptoms: A short CPU hog seen in the ATM PA Helper process when an interface flaps and the framing configuration is modified on the interface.

  Conditions: This symptom is observed on a Cisco 7200 with a PA-A3-T3 adapter that is running Cisco IOS Release 12.2(25)S or 12.2(31)SB (and possibly other Cisco IOS releases).

  Workaround: There is no workaround.

  Further Problem Description: The CPU hog is enough to cause OSPF adjacencies (with fast hello) to go down on other unrelated interfaces. The same problem is seen if BFD is configured.

- CSCin99778

  Symptoms: An ISG configured for RADIUS proxy may see a dummy RADIUS proxy context being created when an accounting stop packet is received.

  Conditions: This symptom is observed when accounting forwarding is configured and an accounting stop comes when no subscriber session exists for that user.

  Workaround: There is no workaround. However, this is a negative case where the ISG receives a stop record before a start record.

- 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 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.

- 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).

- CSCsc47762

  Symptoms: Removal of VRF via “no ip vrf...” in global configuration mode or “no ip vrf forwarding...” in interface configuration mode.

  Conditions: VRF and IP Multicast may be required for the symptom to occur.

  Workaround: Make changes to the startup configuration of the router, and reload the router during a service window.

- CSCsf12539

  Symptoms: Tracebacks may be generated for all accounting messages.

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

  Workaround: There is no workaround.

- 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.

- CSCsg40885

  Symptoms: A router crashes during an online insertion and removal (OIR) of a multilink interface.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured for MLP and PPP.

  Workaround: Shut down the multilink interface before you perform an OIR.

- CSCsg78010

  Symptoms: The **show sss session detailed** command displays traffic for the default traffic class (TC) as “Unmatched Packets (dropped).”

  Conditions: This symptom is observed irrespective of the configuration; for example, whether the default TC is set to forward or drop the traffic.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsi82832

  Symptoms: FastStart does not function on PPP interfaces. (FastStart is enabled by default for regular serial interfaces.)

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2 SB.

  Workaround: There is no workaround.

  Further Problem Description: FastStart acts as a partial solution for the condition that is described in caveat CSCek77555, because FastStart enables an inbound packet from a peer to trigger the startup of PPP (that is, FastStart brings PPP out of the inert state that is documented in caveat CSCek77555).

- CSCsj75575

  Symptoms: A router may crash when applying Dynamic Bandwidth Selection (DBS) parameters to a PPPoE session.

  Conditions: This issue arises only when the **dbs enable** command is configured on an ATM PVC and QoS parameters are applied from RADIUS. This can be reproduced only with one PPPoE PTA session. If the **dbs enable** command is not configured, the crash is not seen.

  Workaround: Disable DBS.

  Further Problem Description: Operational impact.

- CSCsj77305

  Symptoms: A PRE3 crashes if attempts are made to re-establish ISG sessions when CEF IDB is depleted. The **show cef idb** command indicates that CEF IDB is not released when subscriber sessions are all torn down after an HA switchover.

  Tracebacks and error messages of COMMON_FIB-2-IF_NUMBER_ILLEGAL flush on the console during sessions establishment.

  Conditions: This symptom is observed when attempts are made to re-establish ISG sessions when CEF IDB is depleted.

Workaround: There is no workaround.

- CSCsk26165

  Symptoms: A router may crash because of a bus error.

  Conditions: The router must be configured for L2TP.

  Workaround: There is no workaround.

- CSCsk48319

  Symptoms: The control policy rule cannot match a specific class map for the event of credit-exhausted. Debugs show no match for the rule. Only if you use "always" in the class type control for the event credit-exhausted can the rule be applied.

  Conditions: This symptom is observed when a credit exhaust event is configured for a prepaid service.

  Workaround: There is no workaround.

- CSCsk51490

  Symptoms: When attribute 31 and TC (per service) are configured, NO CSID is sent on accounting record for IP sessions.

  Conditions: This symptom is observed with an IP session with TC services and attribute 31 configured.

  Workaround: There is no workaround.

- CSCsk70446

  Cisco IOS emits the %DATACORRUPTION-1-DATAINCONSISTENCY error message whenever it detects an inconsistency in its internal data structures.

  A traceback appears after the error message. This traceback is encountered with long URLs.

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

- CSCsk87523

  Symptoms: The state of the AAA server always shows UP, even when the interface connected to the server was shut down (cnx port is shut (admin down)).

  Conditions: This symptom is observed when the following CLI is configured on the NAS:

  radius-server host *ip-address* **auth-port 2295 acct-port 2296 test username** *username* **idle-time 1 key cisco**

  With this CLI configured, the NAS requests are sent to the server, and then disconnecting the interface connected to the AAA server from the NAS, and when issuing the **show aaa servers** command, the state of the AAA server is shown as UP/DOWN.

  Impact: Display issue.

  Workaround: There is no workaround.

- CSCsk88637

  Symptoms: OAM cells are not generated when a new ATM subinterface and PVC are configured. Subinterface status is up/up; PVC is down. No debug output is seen with the **debug atm oam interface atmx/x.xxx** command.

  Conditions: This symptom is observed when a new ATM subinterface and PVC are configured.

  Workaround: Execute the **shut/no shut** commands on the ATM subinterface.

- 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.

- CSCsk94472

  Symptoms: Service level accounting will not install on a TC session, and no error message will be generated. No failure will be generated, and the TC session will remain established.

  Conditions: This symptom is observed on any TC session with service accounting. This applies to both IP and PPPox parent sessions.

  Workaround: There is no workaround.

- CSCsl02927

  Symptoms: With no traffic on a PA-A6-OC3SMi card, the max ICMP pings times are seen at 352 to 384 ms when testing to an ATM loopback diag. Min/avg are 1/4. This is seen with 1500-byte packets.

  Conditions: This symptom is observed with a 7206vxr backplane version 2.8- 2.11 with the PA-A6-OC3SMi ATM card.

  Workaround: There is no workaround.

  Further Problem Description: This symptom is not observed with version 2.8- 2.11 with the PA-A3-T3 card.

  ```
  Sending 200, 1500-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
  !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! Success rate is 100
  percent (200/200), round-trip min/avg/max = 1/3/352 ms Router# ping 10.1.1.1 repeat
  200 size 1500
  ```

- CSCsl05874

  Symptoms: A Cisco router that is configured with MPLS might have problems forwarding MPLS packets if fragmentation of these packets is required.

  Conditions: This symptom is observed on a Cisco 7200 with NPE-G1 that is running Cisco IOS Release 12.2(31)SB6 and SB7 but could be present in other platforms and releases.

  If the router needs to send large MPLS packets, the issue might appear when the router needs to fragment them (due to MTU constraints).

  Impact: Traffic broken for large packets.

  Workaround: There is no workaround.

- CSCsl20044

  Symptoms: PVC stays INACTIVE when doing PRE switchover with ATM APS.

  Conditions: The primary ATM card of the APS pair is shutdown and then no shutdown. And a PRE switchover is done. Now the ACTIVE APS circuit shows the ATM PVCs as DOWN. Sending traffic over these ATM PVCs can generate the message “%C10K-2-BADRSRCNUM: Invalid resource number from PXF.”

  Workaround: There is no workaround.

- CSCsl21948

  Symptoms: The **show ip subscriber dangle** command may cause a crash.

  Conditions: This symptom is observed in Cisco IOS Release 12.2(31)SB01 and later releases when there are dangling IP sessions.

  Workaround: There is no workaround.

- CSCsl27077

  Symptoms: A system crash may occur during the start of a PPPoA ISG session because of a bus error.

  Conditions: During the start of a PPPoA session with an ISG configuration, Cisco IOS software may experience a bus error and a subsequent crash while processing the access-accept from the RADIUS server. The access-accept will include ISG services to be started on the session indicated by VSA 250 RADIUS attribute-value pairs.

  Workaround: This is a very rare instance, and there is no workaround.

- CSCsl28246

  Symptoms: More than 32,768 TC sessions cannot be brought up, and an "Out of IDs" AAA traceback message is displayed.

  Conditions: This symptom is observed under TC sessions.

  Impact: Traceback preventing scale of ISG PPP Traffic Class. Scalability issue.

  Trigger: While running ISG sessions with PPPoL2TP LAC/LNS on a Cisco 10000, unable to bring up more than 32,768 TC sessions because of the following "Out of IDs" AAA traceback message:

  ```
  Nov 13 11:00:56.696 EST: %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!)
  ```

  AAA is allocating only 1024*32 = 32,768 IDs. Not able to bring up any more sessions because of accounting flow ID allocation failure.

  Workaround: There is no workaround. Traffic classes cannot scale beyond 32,768.

- CSCsl44236

  Symptoms: Duplicate multicast packets are observed on some interfaces in the multicast output list. Packets are replicated twice on some interfaces.

  Conditions: If the interface that has an incoming multicast stream also appears in the output list of the mroute, there could be duplicate packets on some interfaces forming the output list.

  Workaround: There is no workaround.

- CSCsl45783

  Symptoms: CPUHOGs are seen for 16,000 PPPoEQinQ sessions while traffic is being passed.

  Conditions: This symptom is observed when there are 16,000 sessions over 16,000 PPPoEQinQ subinterfaces and when those sessions have L4R configured over them.

  Workaround: There is no workaround.

- CSCsl47915

  Symptoms: Redistribution from OSPF into RIP using a route map based on a prefix list may not work for some routes. The **show ip route** *network* command shows that a network is not advertised by RIP.

  Conditions: This symptom is observed when the prefix list is changed. The RIP database is not updated with the new network that was added to the prefix list.

  Workaround: Issue the **clear ip route** *network* command.

- CSCsl47953

  Symptoms: Bursts of blank lines can be interspersed within the output from the **show memory process** command.

  Conditions: The issue appears to be restricted to the output of this particular **show** command. The output may be influenced by other CLI commands being executed on the router.

  Workaround: Avoid executing any commands on the router during the one-hour time period used to collect the output from the CLI **show** command.

- CSCsl61127

  Symptoms: An NSE-150 reloads unexpectedly when the **show pxf crash** command is entered.

  Conditions: Router is running Cisco IOS Release 12.2(31)SB3 or a later rebuilt.

  Workaround: Do not use the **show pxf crash** command. Cisco IOS Releases 12.2 (31)SB2 and earlier releases are not affected.

- CSCsl61225

  Symptoms: An NSE150 reloads because of a PXF crash on TMC1, Col 1, Row 2.

  Impact: Operation of the network since router is loading.

  Conditions: This symptom is observed when the router is running Cisco IOS Release 12.2(31)SB8.

  Trigger: The crash is due to misaligned network_start. The concerned interfaces are tunnel204 and gig0.205. QoS pre-classify is configured on the tunnel.

  Workaround: There is no workaround.

- CSCsl63197

  Symptoms: A Cisco 10000 platform that is acting as an LNS crashes by bus error.

  Conditions: The crash is seen in Cisco IOS Release 12.2(31)SB10 when the Cisco 10000 is applying the QoS configuration for the users.

  Workaround: There is no workaround.

- CSCsl67817

  Symptoms: When you have maximum channels configured on a chstm1/choc12 card with more channels configured on ct3 card, the ac mgr process on the standby goes high during configuration download.

  Conditions: This symptom is observed during configuration loads and link flaps.

  Workaround: There is no workaround.

- CSCsl68031

  Symptoms: PPPoE sessions fail to come up.

  Conditions: This symptom is observed only when an RBE and PPPoE are configured on the same ATM subinterface.

  Workaround: Configure the **no service pppoe-spoof-detect** command to bring up a PPPoE session.

- CSCsl70617

  Symptoms: A user cannot use the redundant card once the router is reloaded with an APS configuration.

  Conditions: Configure APS, reload the routers, and disassociate cards that are attached through APS CLI. Now the user cannot use the redundant card; sessions will not come up on that card.

Workaround: Enter a **no card** command followed by a **card** command to get the card back into a functional state.

- CSCsl74441

  Symptoms: "%INTERFACE_API-3-NODESTROYSUBBLOCK: The SWIDB subblock named SW FIB PENDING EVENT was not removed" error messages are observed on the router. This symptom does not affect traffic but may be the cause of a memory leak.

  Conditions: This symptom is observed when PPPoE/L2TP sessions are established on Cisco 7300 routers. CSCsk38385 addresses this issue on Cisco 7200 routers.

  Workaround: There is no workaround.

- CSCsl77525

  Symptoms: Downstream PPPoE session traffic over an ATM VC on an LNS is not shaped according to the applied policy map.

  Conditions: This symptom is observed on standard PPPoEoA LNS session configurations. Passing traffic downstream and applying an HqoS policy on the egress interface, the session traffic is not shaped by the shaper configured on the VC.

  Workaround: There is no workaround.

  Further Problem Description: The shaping failure is the result of an output packet queue for the shaped traffic using the ATM subinterface instead of the ATM PVC.

- CSCsl86206

  Symptoms: This problem is internal only; it will not affect any functioning of the router; and it has no associated symptoms.

  Conditions: The user would need to have a queueing policy map applied to an LNS session and then remove that policy map and replace it with a non- queueing policy map to create this case.

  Workaround: There is no workaround.

- CSCsl87935

  Symptoms: Memory leak in SSS. SSS info element and SSS info list.

  Conditions: QoS fails being deleted from the session and reports the failure to Session Manager (SM). Session Manager finishes cleaning up the session.

  Workaround: There is no workaround.

  Further Problem Description: When the TC feature is being deleted, it will send this SSS_INFOTYPE_SERVICE_REMOVED_KEY element key to SM in a notify event. By this time, SM has finished clearing this session and therefore cannot locate the SM context. SM will, in turn, display an error message:

  ```
  Jan 17 09:28:31.816: SSS MGR: Bad Handle in Feature Msg, ID = 0x37000002
  ```

  And return without cleaning up both message and any transient data within the message.

- CSCsl98665

  Symptoms: Multilink bundles fail to come up.

  Conditions: This problem will be seen only if the bundle has 10 members associated with it.

  Workaround: Remove one member from the bundle, by removing the **ppp multilink group** command, and then do a **shut/no shut** of the bundle.

  Further Problem Description: If we try to bring up a bundle that has 10 members, the bundle will fail to come up. If the bundle has less than 10 members, we will not see this issue.

- 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.

- CSCsm01704

  Symptoms: A Cisco 10000 may see high CPU and/or CPUHOG error messages when doing a lawful intercept tap. This may also happen with an ACL configuration change that causes the ACLs to recompile.

  Conditions: This symptom is observed when the tap and access lists are on a loopback interface.

  Workaround: There is no workaround.

- CSCsm14007

  Symptoms: ifOutOctets and ifHCOutOctets are 0 and not being incremented for some Virtual Access interfaces.

  Conditions: This symptom is observed on a Cisco 10000 router that is running Cisco IOS Release 12.2(31)SB6.

  Trigger: Unknown.

  Impact: Monitoring and troubleshooting of Virtual Access interfaces using SNMP are impacted.

  Workaround: There is no workaround.

  Further Problem Description: Interface counters as seen in the output from the **show interface** command are incrementing okay. ifInOctets and ifHCInOctets are incrementing. The problem is affecting only some Virtual Access interfaces, not all.

- CSCsm19663

  Symptoms: A router crashes when MPLS VPN configurations are applied.

  Conditions: This symptom is observed with the following configuration:

  Router(config-if)# **interface a1/0.1 point-to-point**
  Router(config-subif)# **mpls ip**
  Router(config-subif)# **mpls label protocol ldp**
  Router(config-subif)# **ip address 10.0.0.2 255.0.0.0**
  Router(config-subif)# **no ipv6 address**
  Router(config-subif)# **ip split-horizon**
  Router(config-subif)# **pvc 6/100**
  Router(config-if-atm-vc)# **encaps aal5snap**
  Router(config-if-atm-vc)# **exit**
  Router(config-subif)# **no shut**

  Workaround: There is no workaround.

- CSCsm23764

  Symptoms: A device keeps reloading every 50 minutes.

  Conditions: The issue will occur only if the standby RP gets reloaded while CEF is part-way through synching initial data to the standby RP before standby hot state is reached in SSO mode.

  Trigger: Removal or reload of standby before CEF initial synch is complete.

  Impact: This issue affects operations.

Workaround: Reload the active PRE if this issue occurs.

- CSCsm27979

  Symptoms: A router crashes with "Address Error (load or instruction fetch) exception" when the **show ip vrf** *vrf-name* command is used.

  Conditions: On one vty session, enter the **show ip route vrf** *vrf-name* command and leave it in the "more" condition. From other user interface session, go to configuration mode, and then enter the **no ip vrf** *vrf-name* command using the same VRF name. After at least 5 minutes, the router will crash after hitting the any key on the session that is doing the **show ip vrf** command.

  Workaround: Make sure that there is no **show ip route vrf** command pending before entering the **no ip vrf** command.

- CSCsm30581

  Symptoms: A BRAS system might experience a crash when applying ACLs downloaded by RADIUS.

  Conditions: This problem can happen during normal system operation and was seen once a week after deploying a special based on Cisco IOS Release 12.2(31)SB10.

  Workaround: There is no workaround.

  Further Problem Description: Another special still based on 12.2(31)SB3 did not show this problem.

- CSCsm31688

  Symptoms: A Cisco 7304 router that has redundant NSE-100 RPs and that is running Cisco IOS Release 12.2(31)SB10 or 12.2(31)SB11 may crash with the following message after a switchover:

```
tmc0 Crash Summary 0040 0300 XHXType :80000000 Global Halt 0040 0308 MACXID :00000008
External Column Memory 3 Exception 0040 0004 IHBXType :00000000 0040 0120 RPXType
:00000000
```

```
%NSE100-3-ERRORINTR: Fatal error interrupt. IOFPGA error interrupt statuses :
Asic/FPGA 0001, Line card 0000, OIR 0000, Envm. 0000
```

  Conditions: The crash will occur only upon inducing a switchover using the **redundancy force-switchover** command and under the following conditions:

  1. Redundancy mode SSO.

  2. Unicast RPF configured on ATM PVCs.

  3. Traffic going out through the PVCs at the time of the switchover.

  The problem does not occur when PXF is disabled (at the time of the switchover) using the **no ip pxf** command.

  Workaround: Disable PXF just before the switchover; enable it once the old primary reloads successfully. This is because that is the window when the crash occurs.

- CSCsm34469

  Symptoms: After a PRE fails over to the standby, and then fails to the standby again, a PPP encapsulation interface bound to a PPP multilink interface that is not active will keep the interface status of the serial link Up/Down.

  Conditions: Three things must be configured on the Cisco 10000 PRE2.

  1. Redundancy mode SSO.

  2. PPP encapsulation.

  3. PPP multilink with the interface created.

  The issue is with PPP multilink and using redundancy mode SSO.

Workaround: Remove the PPP multilink commands from the E1 interface, and remove the multilink interface. Then fail over to the standby.

- CSCsm36630

  Symptoms: A router crashes.

  Conditions: Clearing PPPoE sessions while sessions are coming up with pushing policy maps via RADIUS results in a crash on the Cisco 10000.

  Workaround: There is no workaround.

- CSCsm41685

  Symptoms: The ciscoEnhancedMemPoolMIB table is empty.

  Conditions: This symptom is observed when a Cisco 7301 series router is loaded with Cisco IOS Release 12.2(31)SB11 and when SNMPget(getmany) is performed on the ciscoEnhancedMemPoolMIB.

  Workaround: There is no workaround.

- CSCsm45950

  Symptoms: A BOOTP client does not receive a DHCPOFFER message from the server.

  Conditions: This symptom is observed in Cisco routers that are loaded with Cisco IOS Release 12.5(0.11).

  Workaround: There is no workaround.

- CSCsm47944

  Symptoms: A Gigabit interface on an NSE150 flaps.

  Conditions: This symptom is observed under a high traffic load.

  Workaround: There is no workaround.

  Further Problem Description: This problem is usually caused by defective hardware (SFP, cable, NSE board). Those were swapped, and the problem persisted.

- CSCsm56753

  Symptoms: Concurrent operations on NVRAM can result in corruption of the configuration register on the secondary PRE3 or PRE4.

  Conditions: Concurrent writes and reads to the NVRAM can cause bad data to be read. In the case of this bug, the configuration register is read while the system configuration is being written, and the wrong value is obtained. With HA, if the bad configuration register value is seen as a change and propagated to the secondary, this can result in a system configured for autoboot having its configuration register changed to 0, leaving the secondary at the ROMMON prompt after a reboot.

  Workaround: There is no workaround.

  Further Problem Description: Concurrent access, such as doing a “show bootvar” to read NVRAM while doing a “write” to write it, can cause this condition.

- CSCsm58612

  Symptoms: A Cisco ISG reloads when subscriber sessions have traffic classes.

  Conditions: This symptom is observed when 1000 to 24,000 sessions go down and come up.

  Workaround: There is no workaround.

- CSCsm62038

  Symptoms: A Cisco 7300 with an NSE-100 crashes.

Conditions: This symptom is observed if you configure a hierarchical policy map with a SET command in the second level. The "set" command is *not* supported in the second level policy in the PXF.

Workaround: Do not configure SET in the second level of a hierarchical policy map.

Further Problem Description: Because it is not a supported configuration, the router will not accept that configuration in the future.

- CSCsm62533

  Symptoms: A Cisco 10000 series router may reload unexpectedly while applying service profiles to sessions.

  Conditions: This symptom is observed when applying services that contain QoS parameters. The service that contains QoS must not be the first service that is applied. The router might display tracebacks that show that the aaa_attr handle is retired.

  Workaround: There is no workaround.

- CSCsm65976

  Symptoms: An MLP PPP session is not installed into the correct VRF.

  Conditions: This symptom is observed when the VRF is configured as peruser or service profile through the "ip:vrf-id ..." "ip:unnumbered ..." VSAs.

  Workaround: Use the following:

  lcp:interface-config=ip vrf forwarding <vrf> lcp:interface-config=ip unnumbered <loopback-interface>

- CSCsm66678

  Symptoms: It is a basic functionality breakage. Packets are not getting policed, so the **show policy-map int** command shows wrong counts. Conform and exceed actions are not being performed.

  Conditions: Policing is not working in the MPLS cloud. 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.

- CSCsm68773

  Symptoms: LFI bundles will not come up.

  Conditions: The commit of CSCsl98665 disturbed the single member bundle creation.

  Workaround: There is no workaround.

- CSCsm70714

  Symptoms: A Cisco 10008 PRE2 that is running an engineering special based on Cisco IOS Release 12.2(31)SB10 crashes and reloads because of a bus error.

  Conditions: The Cisco 10000 has the following number of users:

  - PPPoE: 4308
  - VPDN: 926

  Workaround: There is no workaround.

- CSCsm73365

  Symptoms: An ISG does not unapply the "credit-exhausted" service (i.e., the one that was applied upon event "credit-exhausted") if redirect was upon service-name matching.

  Conditions: The step-by-step procedure is as follows:

  Problem Case:

  QT=0 , IT >0 apply L4RD , L4RD is NOT removed upon reauthorization , QT>0 , IT>0 Default-service installed

  ```
  !
  class type control cm-DEF_Inet event credit-exhausted
    1 service-policy type service name DEF_Inet_L4R
  ```

  Workaround: Change the class type control to "always" instead of "cm- DEF_Inet".

  Working Case:

  QT=0 , IT >0 apply L4RD , L4RD is removed upon reauthorization , QT>0 , IT>0 Default-service installed

  ```
  !
  class type control always event credit-exhausted
    1 service-policy type service name DEF_Inet_L4R
  ```

- CSCsm74946

  Symptoms: An (S,G) with low traffic might keep flapping. This (S,G) gets created and then 3 minutes later gets deleted. This (S,G) will keep getting created and deleted based on the traffic.

  This issue can also be seen with an (S,G) corresponding to default MDT in MVPN scenario. This (S,G) will get deleted after 3 minutes but will reappear 30 seconds after the deletion, and the whole cycle continues.

  Conditions: This symptom is observed on a Cisco 10000 that is running Cisco IOS Release 12.2(31)SB9. The traffic rate on this (S,G) has to be less than 1 packet per 10 seconds. The source for this (S,G) has to be a different router.

  In the MVPN case, the Cisco 10000 has to be a PE that is configured for MVPN. In the (S,G), the S is a far-end PE and the G is an MDT group for some VRF. Also the traffic has to be less than 1 packet per 10 seconds.

  Workaround: There is no workaround.

- CSCsm76322

  Symptoms: ISSU fails and numerous issues.

  Conditions: This symptom is observed after the commit of CSCsj77305.

  Workaround: There is no workaround.

- CSCsm78047

  Symptoms: A Cisco ISG is sending both QT and QV in prepaid reauthorization requests even though only time-based prepaid service is enabled. When the billing server responds with QT and QV, the ISG treats it as dual quota and drops the session.

  Conditions: This symptom is observed when the Cisco ISG subscriber is enabled with time-only prepaid service.

  Workaround: If the billing server can always send QV with a very high from beginning to in all reauth responses, then the ISG treats it as dual quota from beginning.

- CSCsm78550

  Symptoms: The reassembly index is not allocated after the bundles are flapped.

  Conditions: This symptom is observed when an MLPoLNS multimember bundle is configured.

  Workaround: To restore the bundle, enter the **clear vpdn tunnel l2tp all** command or the **clear ppp interface** command.

- CSCsm80616

  Symptoms: On a system where the **access-list compiled** command has been configured to enable Turbo ACL or on systems where Turbo ACL is always enabled, increased CPU utilization may be experienced because of Turbo ACL compilations being performed repeatedly.

  Conditions: This symptom has been observed on a Cisco 7300 router (NSE100) that is running Cisco IOS Release 12.2(31)SB8.

  This situation occurs only in rare circumstances based on the traffic received since the system booted. When this issue occurs, the output of the **show processes cpu** command may indicate that the “TurboACL” process is consuming a significant percentage of the CPU time, and in the output of the **show access-lists compiled** command, the “builds” counter increases quickly, approximately one or more times per minute. Additionally, in the pairs of values separated by slashes on the lines labeled “L1,” “L2,” and “L3” in the output of this command, for at least one of the pairs, the value to the left of the slash will be 90 percent or more of the value to the right of the slash.

  Workaround: Note that it is expected that a number of builds will occur in quick succession when the system first starts receiving traffic. If the situation occurs, it will generally stop occurring after some time as additional traffic flows are received; but it may be possible to configure the **no access-list compiled** command followed by the **access-list compiled** command to stop the repeated recompilations.

  However, on some systems, such as the Cisco 7304 router, the **access- list compiled** command is not available. Therefore, Turbo ACL cannot be switched off on the Cisco 7304 because the classification table generated by Turbo ACL code is used by QoS, NAT, and Security ACL to index into their own respective tables. That is the way these features have been designed on the Cisco 7304. On such systems, no workaround is available.

- CSCsm83777

  Symptoms: An address error crash occurs while running Cisco IOS Release 12.2 (31)SB11. Decodes indicate a Layer 4 redirect.

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

  Workaround: There is no workaround.

- CSCsm86753

  Symptoms: Traceback using redirection.

  Conditions: Using redirection in ISG.

Workaround: There is no workaround.

- CSCsm87206

  Symptoms: An alternate PVC may go down if you reload the local PE line card 10 seconds after the remote PE line card.

  Conditions: This symptom is observed with a Cisco 12000 router that is loaded with a Cisco IOS Release 12.0(32)sy0i image. The local PE is configured with 4xCT3, and the remote PE is configured with 1xSTM1 and L2TPv3.

  Workaround: Reload with a long delay between the local and remote PE's LC.

- CSCsm89620

  Symptoms: Billing fails for users.

  Conditions: AAA accounting records are missing attribute 8 for Framed-IP- Address only for stop records of a service profile. The following is an example of what to look for:

  ```
  4d22h: RADIUS(000000FC): Send Accounting-Request to 10.239.89.25:1813 id 1646/176, len 253
  4d22h: RADIUS: Acct-Session-Id [44] 18 “0E00000000000FF5”
  4d22h: RADIUS: ssg-service-info [251] 14 “NO00600_KBF0”
  4d22h: RADIUS: Cisco AVpair [1] 36 “parent-session- id=0E00000000000FE6”
  4d22h: RADIUS: User-Name [1] 14 “XXXXXXXXXXXXXX”
  4d22h: RADIUS: Acct-Status-Type [40] 6 Stop [2]
  4d22h: RADIUS: Framed-IP-Address [8] 6 X.X.X.X <<< missing attribute
  ```

  You can tell it is a service accounting record when you see parent-session- id.

  Workaround: Enable AAA accounting for the session as well as for the services.

- 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.

- CSCsm93059

  Symptoms: The card type configuration disappears from active, whereas the corresponding interface configurations still show up. This results in a mismatch of configuration sync to the standby, and the standby is rebooted.

  Conditions:

  - On the new active card, the card type configuration is missing.
  - Insert a card into a new slot that has not been configured earlier with the card type configuration.
  - Remove the card.
  - Do a switchover.
  - On the new active card, the card type configuration is missing.
  - The new standby reboots because of a mismatch.

  Workaround: To avoid the sync mismatch, add the corresponding card type configuration.

  Further Problem Description: This problem was due to a wrong piece of code that used to remove the card configuration (if the earlier inserted card was not present) after a switchover on the new active. Whereas the standby was made to escape this check to take care of another race condition. This caused the configuration sync mismatch, resulting in standby reboot.

- CSCsm95040

  Symptoms: On a ds3atm line card, modifying dsx3mode from plcp to adm or vice versa on one ATM port causes the PVCs on all other ports to go down.

  Conditions: This symptom is observed when dsx3mode is modified from plcp to adm or vice versa.

  Workaround: Remove all PVCs and redefine them, or reload the line card.

- CSCsm98573

  Symptoms: A Cisco 10000 that is running ISG configurations could potentially experience instabilities.

  Conditions: This symptom is observed with releases that have the fix for CSCek50693.

  Workaround: There is no workaround.

- CSCso02075

  Symptoms: When performing a ROMMON upgrade, operations that cause the Cisco IOS software to call ROMMON may cause the PRE3 or PRE4 to crash.

  Conditions: This condition is observed when using the **upgrade rom** Cisco IOS command and performing operations that call ROMMON, including the **show bootvar** command or the **boot system** command.

  Workaround: There is no workaround.

  Further Problem Description: If the board hangs while upgrading the ROMMON, it may be necessary to power-cycle the PRE to regain control of it, and it will likely fall-back to the original rom0 image shipped with the board.

- CSCso04194

  Symptoms: Build Breakage.

  Conditions: Unable to compile legacy_hc_counter.o in 64-bit platform directory.

  Workaround: There is no workaround.

- CSCso04286

  Symptoms: Acct-Octets, Acct-packets, IO and OO attributes are not sent in prepaid accounting records for time-only prepaid service.

  Conditions: This symptom is observed when time-only prepaid service is enabled on the ISG.

  Workaround: There is no workaround.

- CSCso06346

  Symptoms: A Cisco 10000 router may enter a state of virtual perpetual churn in which calls continuously fail to come up.

  Conditions: This symptom is observed during aggressive PPPoA call-in.

  Workaround: There is no workaround.

- CSCso06997

  Symptoms: A router crashes.

  Conditions: This symptom is observed when:

  - The **shutdown** command followed by the **no shutdown** command is issued on the ATM interface to which a suspended policy map is attached.
  - The policy map is deleted.

Workaround: There is no workaround.

- CSCso09680

  Symptoms: GRE tunnels with a certain output policy cannot CEF-switch the punted traffic.

  Conditions: If the GRE tunnel has an output policy with set configured, CEF switching does not work.

  Workaround: Turn off CEF switching on the tunnel interface using the **no ip route-cache cef** command. However, this lowers the router performance.

- CSCso10237

  Symptoms: A router crashes when trying to bring up thousands of PPPoA sessions.

  Conditions: This symptom is observed when there are thousands of PPPoA sessions going up and coming down at the same time. This can happen when all sessions are cleared from the router.

  Workaround: There is no easy workaround. When all PPPoA sessions go down, it is better to bring them up in a phased manner. Shut all ATM interfaces with PPPoA sessions and unshut them one by one.

- 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.

- CSCso17473

  Symptoms: On a Cisco 7300 series router while doing a switchover with the following HSRP configuration, the new secondary router reloads continuously with the following error message.

  ```
  HSRP:Gi0/0.801 Grp 1 RF Encode data descriptor failed
  ```

  Conditions: This symptom is observed in a GLBP/HSRP environment. It occurs only on the native Gigabit Ethernet or Fast Ethernet interface of a Cisco 7300 series router.

  Frequency: Easily reproducible.

  Trigger: Switchover.

  Impact: The standby reloads continuously.

  Workaround: Upgrade the Cisco IOS software.

  The GE/FE ports on the standby NSE-100 and GE ports on the NPE-G100 on the Cisco 7300 do not have SSO capability. That is, these ports will flap when the system undergoes a switchover. Only these interfaces on a Cisco 7300 are affected.

- CSCso24243

  Symptoms: A VC associated with a VT keeps flapping.

  Conditions: This symptom is observed when LFIoATM is configured on a Cisco 7200 or when dLFIoATM is configured on a Cisco 7500 router.

  Workaround: There is no workaround.

- CSCso25079

  Symptoms: When using hierarchical shaping, a class queue in a child policy map (CBWFQ) does not give the minimum guaranteed rate (bandwidth rate).

Conditions:

- This problem occurs on a Cisco 7304 with either NSE100 or NSE150.
- This problem occurs when parent-Shaper is active due to one or more class queues in the child policy map having oversubscribed traffic against the configured bandwidth.
- The class queue does not give the minimum guaranteed rate due to the queue drop. And the queue drop occurs whereas the class queue is not oversubscribed rate.

Workaround: There is no workaround.

- CSCso29879

  Symptoms: In a PRE2, high latency is observed in the MLP bundle link for the *non-priority queue* traffic.

  Conditions: This symptom is observed under the following configurations:

  - Multilink
  - One 64-kbps member link per bundle
  - One priority queue and one or more class queues per bundle
  - Fragmentation and interleave enabled

  Workaround: In global configuration mode, configure both the priority-queue and the non-priority-queue threshold values to 2.

  1. ip pxf bfifo-threshold priority-queue 2

  2. ip pxf bfifo-threshold non-priority-queue 2

  Further Problem Description: CSCso29879 is not a bug, and an option has been provided to manipulate the bundle FIFO queue length for the priority queue and non-priority queue. When the threshold is set to lower values, the latency will be lower.

  Default values for the bundle FIFO threshold for the priority queue and non- priority queue are 6 and 16, respectively. *It is recommended that the bundle FIFO queue threshold be left at the default values.*

- CSCso30598

  Symptoms: If GLBP is configured on the native Gigabit Ethernet interface of a Cisco 7300, the router will continually reload if an HA switchover is performed.

  Conditions: This problem affects only the native Gigabit Ethernet interface of a Cisco 7300 because this hardware does not support HA.

  Workaround: There is no workaround.

- CSCso55114

  Symptoms: An align traceback may be generated on a Cisco 10000 series.

  Conditions: This symptom is observed when a 4-port channelized T3 half-height comes up with a huge configuration.

  Workaround: There is no workaround.

- CSCso73266

  Symptoms: L4-redirect intermittently fails. CoA Nack is returned to the redirection server.

  Conditions: These symptoms can occur in a high-traffic situation in which many requests need to be handled by the ID manager database.

  Workaround: Reload the router running ISG.

- CSCso75907

  Symptoms: In a Cisco 7304 NSE-100, traffic shaping is broken. It is dropping more than 50 percent of the shaped rate.

  Conditions: This symptom is observed on a Cisco 7304 router with an NSE-100 or NSE-150 when an interface is configured with a service policy with parent shaping.

  Workaround: There is no workaround.

  Fix Details: The fix for this issue does not cover CBWFQ with a shaping rate less than 4 mbps. To track this specific case, CSCsq19176 has been filed.

- CSCsq21589

  Symptoms: L4-redirect intermittently fails. CoA Nack is returned to the redirection server. Dangling records (records for non-existent session) exist in the idmgr database.

  Conditions: The conditions under which this symptom is observed are unknown.

  Workaround: Reload the router that is running ISG.

Open Caveats—Cisco IOS Release 12.2(31)SB11

Cisco IOS Release 12.2(31)SB11 is a rebuild release for Cisco IOS Release 12.2(31)SB. This section describes caveats that are open in Cisco IOS Release 12.2(31)SB. There are other open caveats in Cisco IOS Release 12.2(31)SB11. However, open caveats are normally listed only for maintenance releases, and the listing of these caveats is an exception.

IP Routing Protocols

- CSCsl98665

  Symptoms: Multilink bundles fail to come up.

  Conditions: This problem will be seen only if the bundle has 10 members associated with it.

  Workaround: Remove one member from the bundle, by removing the **ppp multilink group** command, and then do a **shut/no- shut** of the bundle.

  Further Problem Description: If we try to bring up a bundle that has 10 members, the bundle will fail to come up. If the bundle has less than 10 members, the issue is not seen.

Resolved Caveats—Cisco IOS Release 12.2(31)SB11

Cisco IOS Release 12.2(31)SB11 is a rebuild release for Cisco IOS Release 12.2(31)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB11 but may be open in previous Cisco IOS releases.

IP Routing Protocols

- 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.

- CSCef82084

  Symptoms: Spurious memory accesses occur on a Cisco 7200 series and ALIGN-3-SPURIOUS error messages are generated.

  Conditions: This symptom is observed on a Cisco 7200 series that processes traffic through a serial interface.

  Workaround: There is no workaround.

- CSCeg25475

  Symptoms: Filtering BGP routes by means of the **distribute-list prefix MARTIAN in** command applied to address-family ipv4, actually filters out M-BGP routes in address-family vpnv4.

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

  Workaround: Use route-maps to filter routes inbound.

  Further Problem Description: It can be checked by means of the **show ip bgp neighbors** command that the prefixes are actually being filtered out from updates for address-family vpnv4, and not for ipv4, as it is configured.

- CSCei93982

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

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

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

  Workaround: There is no workaround.

- CSCek49107

  Symptoms: A router crashes when you unconfigure and then reconfigure MLPoFR.

  Conditions: This symptom is observed on a Cisco router that has a QoS service policy with traffic shaping.

  Workaround: There is no workaround.

- CSCek51676

  Symptoms: Router crashes on watchdog timeout.

  Conditions: This symptom occurs when deleting lots of interfaces with the **interface range** command.

  Workaround: There is no workaround.

- CSCek56693

  Symptoms: When you deactivate an ATM PVC, an “ALIGN-3-SPURIOUS” error message may be generated on the console.

Conditions: This symptom is observed when the ATM PVC is carrying PPPoA sessions.

Workaround: Deactivate the PPPoA sessions before you deactivate the ATM PVC.

- CSCek63384

  Symptoms: A service policy is unexpectedly removed.

  Conditions: This symptom is observed when you apply a service policy to a multilink interface and then the interface is reset.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reconfigure the service policy after the multilink interface has been brought up.

- CSCek74752

  Symptoms: In standby the following commands are not displayed when viewing running configuration:

  connect atom_1 POS4/0 500 l2transport

  xconnect 9.0.0.3 100 encapsulation mpls

  Conditions: This symptom occurs on a Cisco 7600 router.

  Workaround: There is no workaround.

- CSCek74840

  Symptoms: A Cisco 10000 series router may reload unexpectedly with COMMON_FIB-2-IF_NUMBER_ILLEGAL tracebacks.

  Conditions: This symptom was observed when bringing up a large number of mixed PTA and L2TP sessions. The system is on SSO mode of High Availability.

  Workaround: There is no workaround.

- CSCek75931

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

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

  Workaround: There is no workaround.

- CSCek75949

  Symptoms: A Cisco 10000 series router may reload unexpectedly during aggressive PPPoA call bringup.

  Conditions: This symptom is observed in system test on a Cisco 10000 series router that is running Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCek76620

  Symptoms: A Cisco 10000 series router may reload unexpectedly during aggressive PPPoA call bringup.

  Conditions: This symptom is observed in system test on a Cisco 10000 series router that is running Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCek79426

  Symptoms: A Cisco 10000 series router may reload unexpectedly during aggressive PPPoA call bringup.

Conditions: This symptom is observed in system test on a Cisco 10000 series router that is running Cisco IOS Release 12.2SB.

Workaround: There is no workaround.

- CSCsc33350

  Symptoms: By default, dot1q subinterfaces do not report link up/down conditions via SNMP traps. While this can be changed using the **snmp trap link-status** interface configuration command on the subinterface, this command is not retained upon reloading the device.

  Conditions: This problem has been observed on Cisco 1721, Cisco 2620 and Cisco 2621XM routers that are running Cisco IOS Release 12.3(13a), Release12.4(3), or Release 12.3(14.12), but other platforms may also be affected.

  Workaround: Reapply the **snmp trap link-status** interface configuration command after the device has been restarted.

- 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.

- CSCsg04630

  Symptoms: Crash is seen on Standby Route Processor.

  Conditions: The crash is normally seen in case of unnumbered relay, when Standby Relay gets synced from Active Relay. The crash is showing some data inconsistency issue while the Standby Relay gets synced.

  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.

- 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.

- 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.

- CSCsi32575

  Symptoms: The SNMP input and output counters may not be incremented or may show a wrong value.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and a POS interface that is configured for Frame Relay encapsulation.

  Workaround: Do not use SNMP for information about the input and output counters. Rather, enter the **show frame-relay pvc** command.

- CSCsi46184

  Symptoms: Cisco IOS crash is observed when removing PCMCIA flash card.

  Conditions: This crash can occur when the flash card is removed during a read to the card.

  Workaround: Do not remove flash card when it is in use.

- 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.

- 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.

- CSCsj47705

  Symptoms: An accounting record may indicate that the NAS-Port-Id has an adapter number of 1 when the correct adapter number is greater than 1.

  Conditions: This symptom is observed when AAA accounting is configured and a PPP interface that is used as a NAS port has more than two adapters.

  Workaround: There is no workaround.

- CSCsj59130

  Symptoms: A router crashes when QoS is configured on POS and traffic line rate is sent.

  Conditions: This symptom is observed when QoS and above line rate traffic.

  Workaround: Remove QoS.

- CSCsj74403

  Symptoms: A spurious memory access message like this one:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x62228B5C reading 0x18
  %ALIGN-3-TRACE: -Traceback= 62228B5C 61355F34 613560C8 607172BC 60732490 6083976C
  60839758 00000000
  ```

  is displayed on the console of the router when you configure a class map under the frame-relay interface-dlci statement of a MFR bundle and that this class map has not been defined yet, and there is already an output queuing policy attached to an other class map, which is already attached to the MFR bundle.

  Conditions: This symptom happens only if there is already an output queuing policy attached to another class map attached to the MFR bundle and the class map you try to attach does not exist yet.

  Workaround: There is no workaround.

- CSCsj95467

  Symptoms: Local switching connection will not pass traffic after microcode reload in a router.

Conditions: This issue occurs when a user does a microcode reload with local switching connection configured.

Workaround: Delete the connection and configure it again.

- CSCsj99980

  Symptoms: User is not able to configure AToM Xconnects on interfaces that use PA-POS-1OC3 cards. The following error message is displayed:

  ```
  MPLS encap is not supported on this circuit
  ```

  Conditions: Xconnects cannot be configured only when PA-POS-1OC3 cards are used.

  Workaround: There is no workaround.

- CSCsk03521

  Symptoms: When F4 QoS model is configured, that is VLAN is shaped, and PPPoEoVLAN sessions are configured with hierarchical policy-map (top shaping, child PQ/CBWFQ), and traffic is generated, the policy-map attached for VLAN shaping counters show all zeroes. With no broadband case, policy-map attached at VLAN shows counters as non-zeros.

  ```
  pumoni-1#show policy-map int

   TenGigabitEthernet1/0/0.1

    Service-policy output: pm_vlan_shaper

      Class-map: class-default (match-any)
        0 packets, 0 bytes
        30 second offered rate 0 bps, drop rate 0 bps
        Queueing
        queue limit 25000 packets
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 0/0
        shape (average) cir 1000000000, bc 4000000, be 4000000
        target shape rate 1000000000
  ```

  Conditions: This problem is seen with both 10GE and 1GE.

  Workaround: There is no workaround.

- CSCsk07097

  Symptoms: After clearing PPPoEoVLAN session, applying a HQoS policy on the VLAN fails.

  Conditions: This issue occurs on a Cisco 10000 series router with PRE3 board. A session comes up on a VLAN/QinQ, and HQoS is applied to that session. When the session is removed, applying a HQoS policy on the VLAN/QinQ fails.

  This only occurs if the session parent policy is configured with “bandwidth remaining ratio x”.

  Workaround: There is no workaround.

- CSCsk17564

  Symptoms: A Cisco 7200 series may crash when you perform a soft OIR of a port adapter.

  Conditions: This symptom is observed when Frame Relay encapsulation is configured along with QoS on a PA-4T+ port adapter. However, the symptom is not specific to the PA-4T+ port adapter.

  Workaround: There is no workaround.

- CSCsk30326

  Symptoms: COA client sends message to the COA server (BRAS). NAS is unable to identify subscriber session when COA client and subscriber are on different VRFs.

  Conditions: This symptom occurs when the COA client (RADIUS server) is on a VRF which is different from the subscriber sessions VRF.

  Workaround:

  1. Configure COA client on same VRF as subscriber session. Limitation: reconfiguration of VRF required for VRF transfers.
  2. Use PBHK. Limitations: Does not completely separate control management traffic from subscriber environment, this is a security issue.

  Further Problem Description: Fix for the bug allows for specifying the VRF on which subscriber session is present.

- CSCsk32296

  Symptoms: NAS crashes when sending invalid account session ID.

  Conditions: None.

  Workaround: There is no workaround.

- CSCsk32753

  Symptoms: An unexpected PXF crash occurs after showing the following error messages:

  ```
  Sep  2 17:48:20 BST: %C10KEVENTMGR-4-PXF_CRASHINFO: Writing PXF debug
   information to bootflash:pxf_crashinfo_20070902-164820.
   Sep  2 17:48:24 BST: %C10KEVENTMGR-1-MAJOR_FAULT: PXF DMA OQC at End of
   Descriptor With Non-Zero Continuation Bit, Restarting PXF
  ```

  Conditions: This symptom is happening several times in a Cisco 10000 series router that is running Cisco IOS Release 12.2(31)SB6, with no changes or interaction with the box at the moment of the crash. This symptom is seen on a Cisco 10000 series router that is acting as a LNS device in a broadband configuration.

  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.

- CSCsk50168

  Symptoms: A router crashes on removing encapsulation from ATM subinterface when bundle is up.

  Conditions: This symptom is observed on a Cisco 10000 router with MLPoATM/MLPoLNS up.

  Workaround: There is no workaround.

- CSCsk55692

  Symptoms: A Cisco 7500 series router that is running Cisco IOS Release 12.2SB and Release 12.0S continues to witness output drops after configuring and unconfiguring an Output Policy containing Police feature on a Logical Interface. On a Cisco 7507 router that is running Cisco IOS Release 12.0(32) S9, reconfiguring fair-queue causes the VIP crash by signal = 10.

Conditions: The problem is caused when installing a policy with police on a logical interface: Subinterface, ATM PVC, Frame Relay DLCI, etc. After removal of such policy, the interface continues to police traffic. If the interface is configured with FR and the fair-queue is reconfigured, the VIP crashes.

Workaround: There is no workaround. The router has to be reloaded to correct the behavior.

- CSCsk65374

  Symptoms: A Cisco 10000 router may crash when sessions are being established/torn down with sessions using per-user access-lists applied via RADIUS.

  Conditions: This symptom is observed with sessions with per-user ACLs.

  Workaround: There is no workaround.

- CSCsk65796

  Symptoms: All frames received on gigabit ethernet interface are dropped. All drops are reported as overruns in the output of **show interfaces** and **show controllers**.

  Conditions: Symptom is observed on gigabit ethernet interfaces on NPE-G2 network processor of Cisco 7200 Series Routers. All IOS trains that support NPE-G2 are affected.

  Symptom is observed only when the gigabit ethernet controller is in promiscuous mode and with moderate traffic rate. Line protocol on the interface remains up when the error condition is present.

  Workaround: There is no workaround. When the gigabit controller falls into this condition, the only way to recover is to power-cycle the router. Soft reload does not clear the problem.

  Further Problem Description: Ethernet controller goes into promiscuous mode under two conditions:

  - bridging is configured on the interface
  - number of MAC addresses that have to be stored in its MAC address filter table exceed the capacity of the table.

  The latter case may happen when a large number of HSRP groups is configured or a large number of IP multicast groups are to be received on the interface.

- CSCsk65987

  Symptoms: HA sync message handling of InARP map results in buffer overflow copy.

  Conditions: This issue is seen only in HA test scenario and also with large Subif I/F name and large VPI/VCI number.

  Workaround: Use the small number for Subif and VPI/VCI.

- CSCsk83480

  Symptoms: The multilink interfaces are going down while running LFIoFR.

  Conditions: This symptom is seen when configuring LFIoFR. Verify everything is working fine and follow these steps:

  - no encap frame-relay, on the interface
  - encap frame-relay, on the interface
  - configure LFIoFR DLCI, on the subinterface
  - default all configs under virtual-template
  - no int virtual-template 1
  - int virtual-template 1

  - configure back all configurations under virtual-template

  Workaround: There is no workaround.

- CSCsk88269

  Symptoms: A router crashes when scaling to 1000 eBGP sessions and flaps the interfaces.

  Conditions: This symptom happens when there is a lot of hash collisions as routes are deleted.

  Workaround: There is no workaround.

- CSCsk94976

  Symptoms: Outbound L2VPN traffic does not flow over Ethernet interface on Cisco 10000 router.

  Conditions: This symptom is observed when a PE router reloads.

  Workaround: Disable CDP on the interface.

- CSCsl04563

  Symptoms: In Cisco 10000 series router with a two-level policy, adding queue- limit to the class-default of the parent policy is an invalid configuration if the child has queuing features. It should be blocked.

  Conditions: There should be a hierarchical policy-map with child having queueing features like bandwidth, queue-limit, priority. With child policy attached to class-default of parent, adding queue-limit to class-default of parent-policy is an illegal configuration.

  Workaround: There is no workaround.

- CSCsl05546

  Symptoms: Traffic is not flowing after SSO switchover when active APS ATM card is shut on an APS pair.

  Conditions: This symptom occurs after SSO switchover when active APS ATM card is shut on an APS pair. Traffic is not flowing.

  Workaround: There is no workaround.

- 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 4.2.20.0
BGP routing table entry for 100:1001:4.2.20.0/24, version 1342275
Paths: (2 available, best #1, table v1001)
Flag: 0x420
  Not advertised to any peer
  65164, imported path from 100:1:4.2.20.0/24
    192.168.7.7 (metric 4) from 192.168.5.5 (192.168.5.5)
      Origin IGP, metric 1552, localpref 80833, valid, internal, best
      Extended Community: RT:100:1001
      Originator: 192.168.7.7, Cluster list: 192.168.5.5
      mpls labels in/out nolabel/291
  65164, imported path from 100:1:4.2.20.0/24
    192.168.7.7 (metric 4) from 192.168.5.5 (192.168.5.5)
```

```
Origin IGP, metric 1552, localpref 80833, valid, internal
Extended Community: RT:100:1001
Originator: 192.168.7.7, Cluster list: 192.168.5.5
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.

- CSCsl11153

  Symptoms: Tracebacks and the following error message are seen:

  ```
  %SYS-3-INTPRINT: Illegal printing attempt from interrupt level.
  ```

  Conditions: This symptom is observed on a Cisco 7304 router that is running Cisco IOS Release 12.2(31)SB8. QoS is configured. The configuration for a particular policy map total bandwidth is greater than the configured or reserved bandwidth for the interface on which the policy map is applied.

  Workaround: There is no workaround.

  Further Problem Description: Service policy is not applied to the interface as expected, no interruption for the router operation.

- CSCsl21709

  Symptoms: Incorrect Account Name is shown in accounting records when TAL is configured.

  Conditions: This symptom occurs when a service name is pushed onto a session, and no attribute 1 string is configured in the user profile.

  Workaround: Configure an attribute 1 string in the user profile.

- CSCsl22605

  Symptoms: “May_suspend” traceback messages are seen when a child policy is removed:

  ```
  %SYS-2-INTSCHED: 'may_suspend' at level 7
  ```

  Conditions: This symptom occurs with large configurations when there are many interfaces using the same policy.

  Workaround: There is no workaround.

- CSCsl25928

  Symptoms: QoS policy counters do not record all the packets in matching class.

  Conditions: This symptom is observed on a Cisco 7300 series router with NSE- 150 and Cisco IOS Release 12.2(31)SB8.

  Workaround: There is no workaround.

- CSCsl32567

  Symptoms: When executing the **show aaa attribute protocol radius** command, a router that is running Cisco IOS may crash or output junk characters.

  Conditions: This symptom is seen in images beginning with Cisco IOS Release 12.2(31)SB.

  Workaround: There is no workaround.

- CSCsl37493

  Symptoms: PPP renegotiates on the far end router when it receives a CONFREQ from the head end router during a PRE failover on the head end router. SSO state was verified prior to the PRE failover on the head end router.

Conditions: This symptom is observed in Cisco IOS Release 12.2(28)SB4c and Release 12.2(28)SB10. It was also seen in first engineering image Cisco IOS Release 12.2(28)ZX.

Workaround: There is no workaround.

- CSCsl38866

  Symptoms: Router crashes when scaling to 2000 eBGP sessions.

  Conditions: This symptom occurs when route tables are deleted and inserted frequently.

  Workaround: There is no workaround.

- CSCsl44170

  Symptoms: Lawful Intercept tapped PPPoE LCP/PPP control packets originating from the router contain incorrect payload.

  Conditions: This symptom is observed on a Cisco 10000 router with radius based Lawful Intercept.

  Workaround: There is no workaround.

- CSCsl46799

  Symptoms: VC queues are starved.

  Conditions: This symptom occurs when one or more shaped-UBR VCs experience traffic congestion. The other VCs that are configured on the same port can experience starvation, causing low link utilization on the port. This problem is seen on PRE3 but not on PRE2.

  Workaround: Use unshaped-UBR, CBR or VBR-shaped VCs rather than shaped-UBR.

- CSCsl51829

  Symptoms: The LI tapped PPPoEoA packets show 4 extra bytes for incoming tapped packets and 8 for outgoing tapped packets sent/received over a 4-OC3 ATM port. These bytes are sitting in between the intercept-ID and the SNAP header. Normally, the intercept-ID should be followed immediately by SNAP header.

  Conditions: This symptom is observed on a Cisco 10000 series router with 4-OC3 ATM port, and QoS service is applied via ISG.

  Workaround: Do not have the QoS service applied via ISG.

- CSCsl52481

  Symptoms: Multilink interfaces fail to come up for LFIoFR after router bootup.

  Conditions: Multilink bundles fail to come up for LFIoFR configuration.

  Workaround: There is no workaround.

- CSCsl54889

  Symptoms: When ISG is configured as a DHCP relay and the DHCP client is rebooted or if the DHCP client sends a DISCOVER packet in error, ISG is unable to process subsequent DISCOVER packets.

  Conditions: This symptom occurs when ISG is configured as a DHCP relay, and the DHCP client is either rebooted or sends a DISCOVER packet in error.

  Workaround: Configure ISG as a DHCP server.

- CSCsl55732

  Symptoms: A Cisco 10000 series router may reload unexpectedly during aggressive PPPoA call bringup.

Conditions: This symptom is observed in system test on a Cisco 10000 series router that is running Cisco IOS Release 12.2SB.

Workaround: There is no workaround.

- CSCsl56934

  Symptoms: Summary address is not advertised via virtual-access interface.

  Conditions: This symptom is observed when connecting and disconnecting the sessions.

  Workaround: There is no workaround.

- CSCsl70591

  Symptoms: A router crashes when IPv6 tables have a large number of entries. A traceback can also be seen.

  Conditions: This symptom is seen when IPv6 route tables have a large number of entries. If we delete and insert routes in large number, like flapping interface and flapping BGP sessions, we may experience a router crash or traceback.

  Workaround: There is no workaround.

- CSCsl76601

  Symptoms: Standby PRE goes to hung state. Active PRE is not able to reset the Standby.

  Conditions: This symptom occurs when **hw-module |pre {a|b}| shut** is configured or the **hw-module standby reset hold** command is issued in Active PRE.

  Workaround: Reload of Active PRE.

- CSCsm00979

  Symptoms: The throughput of the ATM PVCs is lower than expected.

  Conditions: This symptom occurs on a Cisco 10000 router with PRE3 RP board if the user has configured a low burst value on a high speed VC.

  Workaround: Configure a higher burst value for the VC.

- CSCsm03235

  Symptoms: Packet statistics are not shown in the queue on a LAC session.

  Conditions: This symptom is seen on a Cisco 10000 router after a PFX microcode reload only.

  Workaround: There is no workaround.

- CSCsm04442

  Symptoms: Delete an interface which has **ip summary-address rip** configured. The router crashes.

  Conditions: In the scenario where different summary addresses are configured for different interfaces, if we delete an interface that has a summary-address configuration which is the last one for that summary-address that it leads to.

  Workaround: Remove the **ip summary-address rip** configuration from an interface which is going to be deleted.

- CSCsm04843

  Symptoms: PXF crashes seen with TCAM parity errors.

  Conditions: These crashes will happen when:

  1. The parity error happens at an invalid entry.
  2. Multiple parity errors happen within a very short time.

Workaround: There is no workaround.

- CSCsm12664

  Symptoms: Feature push for VRF-tx does not work.

  Conditions: On the service profile, a “vrf-id=...” is configured. this is pushed onto a session. This attribute is ignored.

  Workaround: Instead of doing the push through the RADIUS server, do the push using the SESM.

- CSCsm13263

  Symptoms: The router may crash with a bus error while executing the **show ip arp** *interface-name* command.

  Conditions: This symptom occurs when two executive processes are initiated by two different telnet sessions. One process is doing **show ip arp** *interface* while the other process is doing **no ip address** or **ip address** *ip address* under the configuration mode. Both commands are accessing the same interface. There is a chance that the **show ip arp** command will cause the system crash.

  Workaround: Execute the **show ip arp interface** command and the **ip address** command configuration sequentially.

- 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.

- 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.

Resolved Caveats—Cisco IOS Release 12.2(31)SB10

Cisco IOS Release 12.2(31)SB10 is a rebuild release for Cisco IOS Release 12.2(31)SB2. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB10 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsg39295

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

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

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

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

- CSCsk21987

  Symptoms: Missing interim accounting requests for Traffic Class.

  Conditions: When the interim accounting is configured and with the Traffic class attribute.

  Workaround: There is no workaround.

- CSCsk67272

  Symptoms: CPU HOG is reported because of SNMP engine while processing GetBulk of ciscoMemoryPoolEntry.7.3.

  Workaround: Exclude ciscoFrameRelayMIB from polling if applicable.

Interfaces and Bridging

- CSCsk18909

  Symptoms: A Cisco 7200 series that is configured for ATM and QoS may crash.

  Conditions: This symptom is observed when you attempt to change the priority parameters while traffic is being processed.

  Workaround: There is no workaround.

- CSCsk46486

  Symptoms: The Gigabit controller of NPE-G2 board seems to not correctly recognize the QinQ encapsulation, dropping the packets as giants.

  The packets with the double encapsulation above 1496 bytes are not passing through, being dropped at the input of the NPE-G2 as giants.

  Reverting to single encapsulation on both sides the behavior returns as expected, allowing the ping with any size.

  The DF-bit has never been used during the tests.

  Conditions: This symptom is observed on a Cisco 7200 series router that is running Cisco IOS Release 12.2(31)SB7.

  Workaround: Configure the L2 interface MTU to 1504 instead of 1500.

IP Routing Protocols

- 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.

- 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.

- 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.

- 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.

- CSCsj32013

  Symptoms: A Cisco 12000 series router that is running Cisco IOS Release 12.0(32)SY0f code may crash unexpectedly in a customer environment.

  Workaround: There is no workaround.

- CSCsk37659

  Symptoms: Virtual subinterfaces which result from PPP over ethernet sessions will not result in the required connected-routes to appear in the IP routing table. This causes connectivity failure for customer customers.

  Workaround: Execute the **clear ip route *** command or targeted **clear ip ro** commands will cause the routes to appear, but this is not an acceptable workaround in the field.

Miscellaneous

- CSCee47026

  Symptoms: The ATM HA process may crash.

  Conditions: This symptom is observed on a Cisco router that has VCS configured with local switching.

  Workaround: There is no workaround.

- CSCek78330

  Symptoms: A router that is configured with ATM PVCs may generate the following type of error messages:

  ```
  %COMMON_FIB-3-FIBIDBINCONS2: An internal software error occurred. Virtual- Access2.1
  linked to wrong idb Virtual-Access2.1
  ```

  Conditions: This symptom is observed on a Cisco router that has virtual-template subinterfaces.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, enter the **no virtual-template subinterface** command, save the configuration to the startup configuration, and reload the router.

- CSCek79326

  Symptoms: The Cisco 10000 has its standby restarted by itself 5 minutes after booting.

  Conditions: This symptom is observed when the system is in progress to standby cold-bulk. The high availability mode is SSO.

  Workaround: There is no workaround.

- CSCek79456

  Symptoms: A Cisco 10000 does not display forwarding packets in Sampled Netflow. Only terminating packets are shown.

  Conditions: With the **show flow-sampler** and **show ip cache verbose flow** commands, forwarding packets are not counted in these commands.

  Workaround: There is no workaround.

- CSCsc65165

  Symptoms: A Cisco 7200 series reloads unexpectedly when you enter the **hw-module slot** *slot-number* **stop** command for a T3 port adapter.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with 100 EzVPN IVRFs on a DS3 interface of the T3 port adapter.

  Workaround: There is no workaround.

- CSCsg40425

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

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

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

  Workaround: There is no workaround.

- 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.

- CSCsh76558

  Symptoms: The CLI command **show stacks** on any router platform that uses IPC may show a process whose name appears to be corrupted, including a very large number of blank lines before the next line of the **show stacks** output is printed.

  Conditions: The problem is seen when a **show stacks** is issued, or any other command that causes this to be executed (i.e., **show tech-support**, etc.). This is seen in router platforms that have IPC processes.

  Workaround: There is no workaround.

- CSCsi00416

  Symptoms: Router may crash if the **sh ppp mul** command is issued repeatedly.

  Conditions: When the multilink status changes while the **sh ppp mul** command is issued.

  Workaround: There is no workaround.

- CSCsi11314

  Symptoms: After a forced switchover has occurred, ATM subinterfaces may not forward certain packets.

  Conditions: This symptom is observed on a Cisco 7304 that has redundant NSE-100 route processors and that is configured for Reverse Path Forwarding (RPF). The symptom occurs only for ATM subinterfaces on which PVCs are configured.

  Workaround: Disable RPF.

- CSCsi43776

  Symptoms: Some CLI commands on any router platform that supports ISSU and uses IPC may show a.uses IPC may show a process whose name appears to be corrupted, including a very large number of blank lines before the next line of the place where the process name would be printed.

  Conditions: This symptom is seen in router platforms that have ISSU related IPC process. The bug id CSCsh76558 fixed this issue for the **show stacks** command. This bug tracks a more generic fix.

  Workaround: There is no workaround.

- CSCsi58960

  Symptoms: Channelized line cards may reload unexpectedly and an MR-APS failover occurs.

  Conditions: These symptoms are observed on a Cisco 10000 series when packets with a source address of 127.xxx are being processed, causing a PXF crash that triggers a PRE switchover.

  Workaround: Configure an access control list (ACL) to block packets with a source address of 127.xxx.

- CSCsi62498

  Symptoms: A Cisco 7304 PXF crashes every 10-60 minutes after upgrading from Cisco IOS Release 12.2(28)SB5 to Release 12.2(31)SB3.

  Conditions: Issue detected on Cisco 7304 (NSE100) that is running Cisco IOS Release 12.2(31)SB2 or Release IOS 12.2(31)SB3. The crash occurs when these conditions are met:

  - PXF receives packets having TTL=0.
  - The PXF generated ICMP Time Exceeded Response is punted to the RP as there is no adjacency to the source.

  Workaround: There is no workaround.

- CSCsi94792

  Symptoms: GLBP on a Cisco 7304 with 2xNPE-G100 remains stuck in Init after a switchover when SSO-GLBP is enabled (which is the default). The issue does not happen when “no glbp sso” is configured. The stuck in Init state can be cleared by a “shut/no shut” on the interface.

  Conditions: This is seen on a Cisco 7304 with 2xNPE-G100.

  Workaround: Disable SSO-GLBP with “no glbp sso” and glbp will run the reelection process upon SSO switchover.

- CSCsj13565

  Symptoms: CISCO ESR10008 implemented as a Broadband Remote Access Server (BRAS) for PPPoX customers will deplete all available IP address in any ip local IP address pool.

  The **show ip local pool** *pool_name* command will report:

  ```
  Inuse IP addresses and username but no actual Virtual Access interface
  associated..Inuse addresses:
  10.8.7.196 username@cisco.com
  10.8.7.197 username@cisco.com
  10.8.7.198 username@cisco.com
  10.8.7.199 username@cisco.com
  10.8.7.200 username@cisco.com
  10.8.7.202 Vi2.7545 usernaem@cisco.com
  ```

  Conditions: This is observed with Cisco IOS Release 12.2(31)SB5.

  The Customer Premise Equipment (CPE) requires several PPP handshakes (per 3-8sec time period) before finally establishing.

  Virtual Router Forwarding (VRF) is assigned via a Radius Server.

  Workaround:

  1) Remove and reconfigure the ip local pool definition in the router global configuration.

  2) Disable VRF assignment via Radius.

- CSCsj21036

  Symptoms: On Cisco 7304 platform, for ATM Card (PA-A3 and PA-A6) both vbr-rt and cbr cli is missing (not supported).

  Workaround: There is no workaround.

- CSCsj37160

  Symptoms: Cef adjacency is going incomplete after the pcr on the pvp is changed on an ATM interface. CE router is getting 50% packet loss when pinging to remote CE. CE router pings the PE router no packet loss.

  ```
  Conditions: Problem is found in Cisco IOS Release 12.2(31)SB5.
  Trigger
  Config t
  interface ATM1/0
  atm pvp 11 3000 << change
  sh ip cef vrf Internet det | incl com
  Adj source: IP adj out of ATM1/0.44604, addr x.x.x.x (incomplete)
  ```

  Workaround: Clear adjacency or shut/no shut on ATM interface

- CSCsj53517

  Symptoms: Cisco 10000 is caused to crash when ATM card installed (with or without traffic running through card) and card is Pulled.

  Crash also occurs when **hw-module slot reset** command is issued.

  Conditions: Crash occurs when using 1000+ multilink interfaces.

  Workaround: Can avoid the problem by shutting down interfaces then the card before pulling. (Please Note: This does not always work)

- CSCsj88665

  Symptoms: A device with a PA-MC-2T3+ may reset because of a bus error if a channel group is removed while the **show interface** command is being used from another telnet session at the same time, and then the telnet session is cleared. The device may also display Spurious Memory Accesses.

  Conditions: These symptoms have been observed in the latest Cisco IOS 12.4T and 12.2S releases.

  Workaround: Do not remove a channel group while using the **show interface** command for that interface.

- CSCsj93012

  Symptoms: A Cisco 7500 router may crash in QoS code.

  Conditions: ATM, serial interfaces have QoS configurations as output/input policy, and when peer is reloaded.

  Workaround: There is no workaround.

- CSCsj97772

  Symptoms: When deleting a policy-map that is associated with 32,000 PPPoEoQinQ PTA sessions, the Cisco 10000 PRE3 experiences a bus error.

  Conditions: The bus error is seen when using a Cisco 10000 PRE3 router as a PTA BRAS router for 32,000 PPPoEoQinQ sessions. All 32,000 sessions were attached to a single policy-map definition.

  Workaround: Do not remove a widely used Policy-map from the configuration of a high scale BRAS router when the policy-map is attached to tens of thousands of PPPoEoQinQ sessions.

- CSCsk04970

  Symptoms: There is a memory leak and fragmentation in *Dead* process due to MallocLite. After disabling malloclite, it will be seen as memory allocated to the “Virtual Exec” process in the **show memory allocating-process [total]** command output.

  Conditions: The leak occurs whenever the **show vpdn session [l2tp] [all] username** *username* command is used, and there are many non-matching entries. Memory will be leaked proportional to the number of non-matching usernames (approximately 170 bytes per non-match).

  Workaround: Avoid using the **show vpdn session [l2tp] [all] username** *username* command.

- CSCsk18924

  Symptoms: An NSE-100 crashes after you have applied service policies to approximately 600 VLAN subinterfaces.

  Conditions: This symptom is observed on a Cisco 7304 that has a very large configuration that causes memory exhaustion, for example, 4000 VLAN subinterfaces with nested policy maps that are applied to many of these subinterfaces.

  Workaround: There is no workaround.

- CSCsk22847

  Symptoms: When configuring the command **ATM PVP** *cellid cell rate,* the cell rate automatically sets itself to the maximum.

  When configuring the two commands below:

  ```
  ATM PVP cellid cellrate
  ATM PVP cellid no-f4-mgmt
  ```

  The commands are entered individually, however when you view them using a **show run**, they seem to be merged into one command on one line as below:

  ```
  ATM PVP cellid cellrate no-f4-mgmt
  ```

  Then, when the router is reloaded, even though the configuration is saved, the command is erased as Cisco IOS does not recognize it as a valid command.

  Workaround: There is no workaround.

- CSCsk32680

  Symptoms: In MLPoA, we are not able to add more than one member to the bundle.

  Conditions: This problem is seen only when we have the **ppp multilink group** command configured in the VT.

  Workaround: Configure the **ppp multilink group** command in the ATM interface

- CSCsk45947

  Symptoms: Traffic may fail after an aps manual/force cutover.

  Conditions: This is observed when the router is booted up with configurations, not happening with configurations on the fly.

  Workaround: There is no workaround.

- CSCsk51556

  Symptoms: Line card does not come up.

  Conditions: This occurs when the **hw-module subslot shutdown** command is followed by the **no card command** and the **no hw-module subslot shut** command.

  Workaround: Use the **hw-module slot shutdown** command on a full size card.

- CSCsk56028

  Symptoms: System may crash while applying QoS service-policy.

  Conditions: When using a Cisco 10000 router with PRE3 RP board and Cisco IOS Release 12.2(31)SB, the system may crash when applying a QoS service-policy.

  Workaround: There is no workaround.

  Further Problem Description: The crash has not been seen in the field but was found to be possible in development.

- CSCsk62754

  Symptoms: After PRE3 failover, secondary PRE will continuously reboot.

  Conditions: This occurs at this time, when an ESR-HH-1GE is installed and with minimal configuration.

  Workaround: There is no workaround.

- CSCsk74513

  Symptoms: Multilink interfaces are down while running LFIoATM.

Conditions: The issue is seen with c10k2-p11-mz.122-31.4.13.SB8d.070928 image and not seen with c10k2-p11-mz.122-31.4.13.SB8b image.

Workaround: There is no workaround.

- CSCsk88270

  Symptoms: A router crashes on bootup due to column 3 memory exception.

  Conditions: This symptom is observed on a Cisco 7304 NSE-100 Revision C (or EARLIER) that is running Cisco IOS Release 12.2(32)SR image built between 10/01/2007 and 10/16/2007.

  Workaround: There is no workaround.

- CSCsk90990

  Symptoms: This is not an externally visible issue, there are no bugs/problems associated with this fix.

  Conditions: There are no specific environment/runtime issues that are addressed by this fix.

  Workaround: There is no workaround.

  Further Problem Description: The code has been changed to use a componentized version of the cf-client-ids instead of the branch-specific monolithic version. This will prevent the IDs getting out of sync with the IDs in other branches/platforms/trains and ultimately prevent issues down the road. The two versions of the IDs (componentized vs monolithic) are identical and will not introduce any functionality change at this point.

- CSCsk93354

  Symptoms: A Cisco 10000 (PRE-2) that is running Cisco IOS Release 12.2(31)SB8 with a large (9mb) configuration fails to reach HOT state on the standby PRE due to a CPU hog by the BEM VERIFY process.

  Conditions: This symptom is observed on a Cisco 10000 series router with redundant PREs configured for SSO and large configuration stored on flash disk.

  Workaround: Disable the redundant PRE (for example, “hw-module pre b shutdown”).

- CSCsk94976

  Symptoms: Outbound L2VPN traffic does not flow over GigabitEthernet interface on a Cisco 10000 router.

  Conditions: PE router reload with bidirectional L2VPN and L3VPN traffic.

  Workaround: Disable CDP on the router.

Wide-Area Networking

- CSCee56988

  Symptoms: High CPU usage occurs on a Cisco 7301, and the following error message and traceback are generated:

```
%TCP-2-INVALIDTCPENCAPS: Invalid TCB encaps pointer:
0x0
-Process= "L2X SSS manager", ipl= 0, pid= 69
-Traceback= 0x606E43DC 0x60B9FAC8 0x60BA11C4 0x619F502C 0x619F4A2C
0x619F4D34 0x619F35C4 0x619F4FF4 0x619F6820 0x619F5ED8 0x619F6350 0x619CA1F4
0x619CA6C4 0x619D2524 0x619CABB4 0x619CAFA0
```

Conditions: This symptom is observed on a Cisco 7301 that runs Cisco IOS Release 12.4(5b) with PPTP/VPDN connections after, on a connected platform, rate limiting is changed to MQC policy-based limiting of the bandwidth. Note that the symptom may be release-independent.

Workaround: There is no workaround.

- CSCsk27179

  Symptoms: The user is trying to add a map-class with fragmentation when interface level fragmentation is already configured.

  Conditions:

  1. Frame-relay fragment *frag_size* end-to-end configured on the main interface, no CoS policy. Then try to apply a map-class with a parent shaper policy in a map-class under a dlci.
  2. Parent-child output policy applied to the main interface, fragmentation configured on the main interface

  Workaround: There is no workaround.

- CSCsk84780

  Symptoms: High CPU usage may occur when IPCP is being renegotiated. Eventually, the high CPU usage may cause buffers to be backed up, may cause error message to be generated, and may cause L2TP tunnels to be dropped.

  Conditions: This symptom is observed on a Cisco router when clients renegotiate IPCP unnecessarily. You can verify this situation by enabling the **debug ppp negotiation** command or by configuring RADIUS authorization and then checking the virtual-access interface for the phrase “cloned from: AAA, AAA, ...” (that is, multiple instances of AAA) as identification.

  Workaround: There is no workaround.

  Further Problem Description: You can alleviate the situation somewhat by configuring the NCP Timeout to 15 seconds to disconnect clients that take a long time to renegotiate IPCP. You can also do the following:

  - Increase the hello timers for L2TP and for the receive windows.
  - Configure the timers under the virtual template.
  - Do not configure the **redistribution connected** command under a routing protocol such as (but not limited to) EIGRP, RIP, or OSPF.
  - Ensure that the IP local pools are concise. For example, create one statement for multiple /24s instead of splitting all /24s on single lines, because with single lines, the look-up becomes long and contributes to the high CPU usage.

Resolved Caveats—Cisco IOS Release 12.2(31)SB9

Cisco IOS Release 12.2(31)SB9 is a rebuild release for Cisco IOS Release 12.2(31)SB2. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB9 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsk14633

  This is the Cisco Product Security Incident Response Team (PSIRT) response to a vulnerability that was reported on the Cisco NSP mailing list on August 17, 2007 regarding the crash and reload of devices running Cisco IOS software images after executing a command that uses, either directly or indirectly, a regular expression. The original post is available at the following link:

  http://puck.nether.net/pipermail/cisco-nsp/2007-August/043002.html

  The Cisco PSIRT posted a preliminary response on the same day and is available at the following link:

  http://puck.nether.net/pipermail/cisco-nsp/2007-August/043010.html

  Preliminary research pointed to a previously known issue that was documented as Cisco bug ID CSCsb08386 (registered customers only), and entitled “PRP crash by show ip bgp regexp”, which was already resolved. Further research indicates that the cur rent issue is a different but related vulnerability.

  There are no workarounds available for this vulnerability. Cisco will update this document in the event of any changes.

  The full text of this response is available at http://www.cisco.com/warp/public/707/cisco-sr-20070912-regexp.shtml.

IP Routing Protocols

- CSCsj99269

  Symptoms: With some VPN configurations such as configurations with a multipath import or an import map, the CPU usage of the router may be very high for a long time, even after BGP convergence has occurred.

  Conditions: This symptom is observed on a Cisco router that functions in a highly scaled environment involving several hundred of VRFs and occurs after the router has been reloaded or after a switchover has occurred.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(31)SB8

Cisco IOS Release 12.2(31)SB8 is a rebuild release for Cisco IOS Release 12.2(31)SB2. This section describes caveats that are open in Cisco IOS Release 12.2(31)SB8. There are other open caveats in Cisco IOS Release 12.2(31)SB8. However, open caveats are normally listed only for maintenance releases, and the listing of these caveats is an exception.

Interfaces and Bridging

- CSCsk18909

  Symptoms: A Cisco 7200 series that is configured for ATM and QoS may crash.

  Conditions: This symptom is observed when you attempt to change the priority parameters while traffic is being processed.

  Workaround: There is no workaround.

Miscellaneous

- CSCek49107

  Symptoms: A router crashes when you unconfigure and then reconfigure MLPoFR.

  Conditions: This symptom is observed on a Cisco router that has a QoS service policy with traffic shaping.

  Workaround: There is no workaround.

- CSCsi11314

  Symptoms: After a forced switchover has occurred, ATM subinterfaces may not forward certain packets.

  Conditions: This symptom is observed on a Cisco 7304 that has redundant NSE-100 route processors and that is configured for Reverse Path Forwarding (RPF). The symptom occurs only for ATM subinterfaces on which PVCs are configured.

  Workaround: Disable RPF.

- CSCsk17564

  Symptoms: A Cisco 7200 series may crash when you perform a soft OIR of a port adapter.

  Conditions: This symptom is observed when Frame Relay encapsulation is configured along with QoS on a PA-4T+ port adapter. However, the symptom is not specific to the PA-4T+ port adapter.

  Workaround: There is no workaround.

- CSCsk36549

  Symptoms: When L2 local switching is configured for ATM-to-Ethernet interworking, there may be no connectivity between CE routers even though the L2 VCs are up.

  Conditions: This symptom is observed on a Cisco 7304 only after you have disable and re-enabled the **connect** command for the ATM-to-Ethernet interworking configuration.

  Workaround: Disable the PXF engine. If this is not an option, there is no workaround.

- CSCsk38543

  Symptoms: When one of the member links of a a Fast Etherchannel goes down while the other link remains active, a temporary drop in traffic that passes through the Fast Etherchannel may occur.

Conditions: This symptom is observed on a Cisco router that is configured for ARP and occurs only for large packets. The symptom does not occur with regular-sized packets such as 100-byte packets.

Workaround: Enter the **clear arp** command.

- 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

Resolved Caveats—Cisco IOS Release 12.2(31)SB8

Cisco IOS Release 12.2(31)SB8 is a rebuild release for Cisco IOS Release 12.2(31)SB2. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB8 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCek40060

  Symptoms: RADIUS server authentication may not function for dialup and PPP clients.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.4(7) and that has the **radius-server retry method round-robin** command enabled. The symptom is not release-specific.

  Workaround: Disable the **radius-server retry method round-robin** command. Note that the symptom does not occur in Release 12.3 or Release 12.3T.

- 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.

- CSCsf98394

  Symptoms: When the **initiator radius-proxy** command is enabled on an ISG, extra characters are shown with the identifier in the output of **show sss session** and **show radius-proxy client session** commands.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when the user name has at least 8 characters.

  Workaround: Use a user name with less than 8 characters.

- CSCsj89470

  Symptoms: An LNS that has sampled NetFlow enabled may crash.

  Conditions: This symptom is observed on a Cisco 7200 series that functions as an LNS.

  Workaround: Disable sampled NetFlow. If this is 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.

IP Routing Protocols

- 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.

- CSCsg25995

  Symptoms: Networks do not show in the Multiprotocol BGP (MBGP) table, as can be seen in the output of the **show ip mbgp** command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.2SR, Release 12.4, or Release 12.4T.

  Workaround: Enter the **clear ip bgp** *neighbor-address* command to enable the networks to enter the MBGP table.

- 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.

ISO CLNS

- 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

- 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.

- 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.

- CSCsj72039

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

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

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

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

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

Miscellaneous

- CSCeb78526

  Symptoms: A router that is configured for LAN Emulation (LANE) may reload because of a bus error, and the following error message may appear:

  ```
  System returned to ROM by bus error at PC 0xXXXXXXXX
  ```

  Conditions: This symptom is observed on a Cisco router only when the creation of switched virtual circuits (SVCs) fails.

  Workaround: There is no workaround.

- CSCek49973

  Symptoms: When Multilink PPP (MLP) is configured to use a virtual access interface as the bundle interface and when you apply a service policy with bandwidth guarantees that are higher than the bandwidth guarantees of the virtual access interface, an error message is generated because the service policy is not rejected nor enters the suspended mode.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB and that is configured for MLP and QoS.

Workaround: Add more links to the bundle interface and clear the virtual access interface.

- CSCek71346

  Symptoms: The MPLS forwarding table is not shown on a router, causing packet drops in end-to-end connectivity across the MPLS cloud.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router after a switchover has occurred.

  Workaround: There is no workaround.

- CSCek75986

  Symptoms: Traffic may stop on a GRE tunnel that is configured on a VRF-enabled interface.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PE router after a PRE-3 switchover has occurred.

  Workaround: Reload the PXF engine.

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

- CSCek76933

  Symptoms: A router may crash when you configure an ATM PVC on an ATM point-to-point subinterface.

  Conditions: This symptom is observed on a Cisco router when the ATM point-to-point subinterface is already part of a bundle.

  Workaround: Configure the ATM PVC on an ATM multipoint subinterface.

- CSCek77702

  Symptoms: An IP address that is configured for an IMA bundle on a PA-A3-8T1IMA port adapter may become lost after an online insertion and removal (OIR) of the port adapter.

  Conditions: This symptom is observed on a Cisco 7304 when a PVC is configured on the IMA main interface on the PA-A3-8T1IMA port adapter and when there is continuous traffic.

  Workaround: There is no workaround.

- CSCek79367

  Symptoms: The **xconnect** *ip address vcid* **pw-class** *class-name* command may not be nvgened when it is entered along with the **backup peer** *ip address vcid* **pw-class** *class-name* command, and the parser submode "cfg-if-atm-l2trans-pvc-xconn" may not be entered.

  Conditions: This symptom is observed on a Cisco 7304 that has an ATM interface when the encapsulation on the L2transport VC is ATM adaptation layer 0 (AAL0).

  Workaround: There is no workaround.

- CSCsc42938

  Symptoms: A router that is configured for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) may crash when LDP is configured globally or on an interface.

  Conditions: This symptom is observed when you enter the **show mpls ldp neighbor** command while LDP sessions are coming up or going down.

  Workaround: There is no workaround.

- CSCsd28214

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

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

Workaround: There is no workaround.

- CSCse79790

  Symptoms: When PPPoE Relay is configured, only one session comes up successfully. All successive sessions fail. The initiation of more sessions brings down the existing sessions. If there are active sessions that are already existing (not necessarily PPPoE Relay sessions), the initiation of new PPPoE Relay sessions tears down all the sessions.

  Conditions: These symptoms are observed on a Cisco router that functions in a Virtual Private Dialup Network (VPDN). The symptom occurs only for PPPoE Relay sessions and not for normal sessions.

  Workaround: There is no workaround.

- CSCsh87246

  Symptoms: When packets that traverse an IP session are punted to the RP, the RP may read an incorrect MAC address.

  Conditions: This symptom is observed on a Cisco 10000 series when the forwarding adjacency is not resolved for packets that traverse the IP session.

  Workaround: There is no workaround.

- CSCsi05593

  Symptoms: Gigabit Ethernet output counters may become corrupted. When a QoS output policy map is applied while sessions are already up, the counters may show a value that resembles 2^32.

  Conditions: This symptom is observed on a Cisco 10000 series only when the QoS output policy map is used for PPPoEoQinQ sessions and is applied after the router is booted and configured.

  Workaround: Enter the **clear counters** command to reset the corrupted interface counters.

- CSCsi14211

  Symptoms: A CPUHOG condition may occur when an LDP session goes down.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS LDP, that has more than 30 LDP sessions with peers, and that exchanges more than 5000 label bindings for each LDP session. The symptom occurs when the LDP session goes down shortly after it came up.

  Workaround: There is no workaround.

- CSCsi58871

  Symptoms: For a Gigabit Ethernet interface, the ifOutNUcastPkts may decrement rather than increment.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(28)SB but could also occur in Release 12.2S.

  Workaround: There is no workaround.

- CSCsi64528

  Symptoms: A Cisco 10000 series that is configured for QoS may crash.

Conditions: This symptom is observed when you remove a policy map from an ATM interface.

Workaround: There is no workaround.

- CSCsi98901

  Symptoms: The total free count on the secondary policy data index cannot be released after all sessions have been removed. This situation causes memory depletion. After memory has run out for the total free count on the secondary policy data index, tracebacks and error messages such as “The iEdge Toaster Client has been corrupted” and “The iEdge Toaster Client failed to allocate RP Memory” are generated.

  Conditions: This symptom is observed on a Cisco 10000 series only when sessions are constantly brought up and torn down. When the sessions come up and remain up, the indexes are freed when you remove the sessions.

  Workaround: There is no workaround.

- CSCsj07936

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

  1. Symptom 1: When the interface controller functions of an NPE-G2 functions in promiscuous mode, for example, when HSRP is configured, packets that are not destined for the router may be forwarded anyway.

     Condition 1: This symptom is observed on a Cisco 7200 series with an NPE-G2 that runs Cisco IOS Release 12.2(31)SB5 but is not release-specific.

     Workaround 1: If HSRP is configured, enter the **standby use-bia** command. You may need enter the **shutdown** command followed by the **no shutdown** command to change the controller state.

  2. Symptom 2: When BVI is configured on native Gigabit Ethernet interfaces of an NPE-G2 within the same group, a ping may not go through.

     Condition 2: This symptom is observed on a Cisco 7200 series with an NPE-G2 that runs Cisco IOS Release 12.2(31)SB5 but is not release-specific.

     Workaround 2: Configure a static MAC address.

- CSCsj12883

  Symptoms: Frame Relay service policy counters may not be updated.

  Conditions: This symptom is observed on a Cisco 7304 when that has a POS interface that is configured for Frame Relay with a single DLCI that uses an output service policy. The symptom occurs after the following sequence of events:

  1. You create a point-to-point subinterface that is configured for Frame Relay encapsulation, as in the following example:

     ```
     Current configuration: 143 bytes

     !

     interface POS5/0

      no ip address

      encapsulation frame-relay

      load-interval 30

      clock source internal

      frame-relay intf-type dce

     end
     ```

```
mft-73b#sh run int pos5/0.1
Building configuration...

Current configuration : 182 bytes
!
interface POS5/0.1 point-to-point
 ip address 2.2.2.1 255.0.0.0
 snmp trap link-status
 frame-relay interface-dlci 1007
 service-policy input in
 service-policy output out
```

2. You verify the connectivity and service policy outputs by generating traffic. All the QoS counters are updated properly for the service policy on the main interface and subinterface.
3. You remove the point-to-point subinterface, as in the following example:

```
mft-73b#Config t
mft-73b(confgi)# No int  POS5/0.1 point-to-point
```

4. You add the subinterface configuration to the main interface, as in the following example:

interface POS5/0

```
 ip address 2.2.2.1 255.0.0.0
 encapsulation frame-relay
 load-interval 30
 clock source internal
 frame-relay interface-dlci 1007
 frame-relay intf-type dce
 service-policy input in
 service-policy output out
```

5. You generate traffic.
6. You enter the **show policy-map interface** command.

In this situation, the output of the command shows zero for the Frame Relay service policy counters.

Workaround: There is no workaround.

- 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 has 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.

- CSCsj43962

  Symptoms: ISG may send the physical MAC address in ARP reply packets when Gateway Load Balancing Protocol (GLBP) may require the virtual MAC address (VMAC) for proper operation.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, that functions as an ISG, and that connects to another ISG via an interface that is configured for GLBP.

  Workaround: There is no workaround.

- CSCsj54595

  Symptoms: When you add a child policy to a VLAN shaper policy on a subinterface while sessions are active, memory may become corrupted or the router may crash.

  Conditions: This symptom is observed on a Cisco 10000 series when the following sequence of events occurs:

  1. You bring up PPP sessions on a VLAN with an HQoS queuing policy for the sessions.
  2. You attach a flat VLAN shaper to the subinterface while sessions are active.
  3. You attach a child policy to the VLAN shaper policy.

  Workaround: There is no workaround.

  Further Problem Description: In Cisco IOS Release 12.2(31)SB, the router does not crash but memory does become corrupted.

- CSCsj55042

  Symptoms: The ifOperStatus object for a 6-port channelized T3 line card may show that the T1 layer is up while the T3 controller is down. After the T3 controller is shut down, the ifOperStatus object for the controller should show that the T1 layer is down.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for SNMP when the T3 controller of the line card is configured with two T1 links and then shut down.

  Workaround: There is no workaround.

- CSCsj55219

  Symptoms: A Cisco 10000 series that functions as an ISG may reload unexpectedly.

  Conditions: This symptom is observed when the router has 16,000 user connections and when the memory pool is not able to allocate the memory even though memory is available.

  Workaround: There is no workaround.

- CSCsj62499

  Symptoms: The **ip flow-aggregation cache exp-bgp-prefix** command may not show as a supported command because it is hidden.

  Conditions: This symptom is observed on a Cisco 7304 router that has an NSE-100 or an NSE-150 and that runs Cisco IOS Release 12.2(31)SB.

  Workaround: There is no workaround. However, the command is present in the Cisco IOS software image and is accepted when you enter it.

- CSCsj74989

  Symptoms: A PRE-3 may crash when you enter the **show pxf cpu iedge policy detail** command.

  Conditions: This symptom is observed on a Cisco 10000 series while PPPoE over L2TP sessions are coming up.

  Workaround: There is no workaround.

- CSCsj89202

  Symptoms: A memory leak at the SSM connection manager may occur when there are continuous Change of Authorization (CoA) transactions on PPPoE over L2TP sessions. When this situation occurs, the process memory continues to decrease, eventually an "AAA-3_LOW_MEM" error message is generated, and then incoming CoA packets are dropped. The output of the **show aaa memory** command displays the number of dropped CoA packets.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG.

  Workaround: There is no workaround.

  Further Problem Description: When there are no continuous CoA transactions on the PPPoE over L2TP sessions, the memory lead does not occur.

- CSCsj91538

  Symptoms: The input rate on Gigabit Ethernet interfaces shows fluctuating values even when the traffic is constant.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsj94561

  Symptoms: A router may crash because of a bus error when you perform an OIR of a PA-MC-8TE1+ port adapter or when you enter the **hw-module slot** *slot-number* **stop** command for the slot in which the PA-MC-8TE1+ port adapter is installed.

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

  Workaround: There is no workaround.

- CSCsj97211

  Symptoms: Local switching through the PXF engine may not function, preventing local switching circuits from establishing connectivity.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 or NSE-150.

  Workaround: There is no workaround.

- CSCsk11606

  Symptoms: The PXF engine may crash when you tear down a tunnel in an LNS multihop configuration.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an LNS multihop node when you enter the **clear vpdn tunnel l2tp all** on either the LAC or the terminating LNS.

  Workaround: There is no workaround.

- CSCsk18208

  Symptoms: An ISG does maintain the subscriber traffic below the limit that is configured in the "Cisco: Service-Info" of the service profile but the accounting updates report the traffic counters without taking the rate limit into account.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG and occurs only when policing is enabled and traffic counters are configured. For other services such as prepaid services, the symptom does not occur.

  Workaround: There is no workaround.

- CSCsk46465

  Symptoms: The PXF engine on a Cisco 10000 series may crash. When this situation occurs, the following error message is generated:

  ```
  PXF DMA Error - Small Packet Handle Creating a Large Descriptor^M
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a LAC and that has QoS configured when the LNS sends a packet with an inner L2TP packet that is padded to a large number of bytes such that the L2TP packet is much larger than the payload.

  Workaround: Disable QoS on the LAC in the downstream direction.

TCP/IP Host-Mode Services

- CSCek12203

  Symptoms: When you enter the **copy ftp disk** command, the copy operation may fail and cannot be terminated, further **copy** commands may fail, and a TCP vty session for the purpose of troubleshooting the situation may fail and cannot be terminated.

  Conditions: These symptoms are observed on a Cisco platform when the FIN flag is set in the initial ESTAB message from a neighbor. You must reload the router to recover from the symptoms.

  Workaround: Do not enter the **copy ftp disk** command. Rather, enter the **copy tftp disk** command.

Wide-Area Networking

- CSCsi60136

  Symptoms: The standby processor on a router that is configured for PPP may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco router when the **debug ppp redundancy** command is enabled on the standby processor.

  Workaround: Do not enable the **debug ppp redundancy** command on the standby processor.

- CSCsj05288

  Symptoms: When you delete a Frame Relay subinterface, the following error message and a traceback may be generated continuously:

  ```
  SYS-2-BADSHARE: Bad refcount in retparticle
  ```

  Conditions: This symptom is observed on a Cisco router when a Frame Relay subinterface with a service policy is applied inside a VRF.

  Workaround: Recreate and then delete the interface. When you do so, the error message and a traceback are no longer generated.

- CSCsj36201

  Symptoms: The traffic flow stops and tracebacks are generated when the fragmentation size is changed by using an MQC shaped policy on a PVC. When the fragmentation size is set to a value equal to or larger than 700, the router hangs.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.2(31)SB4.

  Workaround: When the symptom has occurred, you must power-cycle the router. To prevent the symptom from occurring, first remove fragmentation, change the size, and then re-apply the map class. To prevent the router from hanging, use FRTS.

- CSCsj93465

  Symptoms: A PRE-3 may crash at the “pppatm_pas_fs” function.

  Conditions: This symptom is observed on a Cisco 10000 series that runs the c10k3-p11-mz image of Cisco IOS Release 12.2(31)SB1 and that is configured for PPP. The symptom occurs after a write operation. The symptom may not be platform-specific.

  Workaround: There is no workaround.

- CSCsk24566

  Symptoms: After a SSO switchover has occurred, a peer router cannot ping the IP address of an MFR interface that is up.

  Conditions: This symptom is observed inconsistently on a Cisco 10000 series only when a MFR interface is created newly and only after the first SSO switchover has occurred.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected MFR interface. Once you have done so, you still can ping the interface after subsequent SSO switchovers have occurred.

- CSCsk31066

  Symptoms: The **ppp mtu pppoe unlimited enhancement** command may not function correctly.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(31)SB7

Cisco IOS Release 12.2(31)SB7 is a rebuild release for Cisco IOS Release 12.2(31)SB2. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB7 but may be open in previous Cisco IOS releases.

Interfaces and Bridging

- CSCsi41769

  Symptoms: A PVC that is shut down by OAM may continue to receive and forward traffic. This situation causes problems in an APS 1+1 redundancy configuration in which the standby router has a PVC that is shut down by OAM but continues to receive all traffic.

  Conditions: This symptom is observed on a Cisco router that has an ATM port adapter.

  Workaround: In an IPv4 configuration, shut down the subinterface manually or enter the **ip verify unicast reverse-path** command. In an MPLS configuration, shut down the subinterface manually.

IP Routing Protocols

- CSCsc74229

  Symptoms: A router may delete the VPNv4 prefixes from the BGP table, even though the counters in the output of the **show ip bgp** command may indicate that the VPNv4 prefixes are present in the BGP table. This situation may cause loss of VPN connectivity.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN and that functions as a PE router.

Workaround: There is no workaround. When the symptom occurs, enter the **clear ip bgp *** command to restore proper operation of the router.

- 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.

- CSCsh51559

  Symptoms: The following error message may be generated on a router that is configured for VPN or VPNv4:

  For VPN:

  ```
  ALIGN-3-SPURIOUS: Spurious memory access made at bgp_vpn_afmodify_walk
  ```

  For VPNv4:

  ```
  ALIGN-3-SPURIOUS: Spurious memory access made at bgp_vpnv4_afmodify_walk
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and IPv4 in a VRF address-family configuration and that imports routes from a VRF.

  Workaround: There is no workaround. However, the error message is of a cosmetic nature and can be ignored.

Miscellaneous

- CSCek73621

  Symptoms: A PA-CC in which a PA-A6 port adapter is installed may crash continuously, preventing the PA-A6 from coming up.

  Conditions: This symptom is observed on a Cisco 7304 after you have entered the **no shutdown** command on an interface of the PA-A6 port adapter.

  Workaround: There is no workaround.

- CSCse41999

  Symptoms: For PPPoEoE sessions on a Cisco 10000 series, the output of the **show interface virtual-access** command shows numbers for received packets and bytes that are double the actual numbers.

  Conditions: This symptom is observed only for PPPoEoE packets that are punted to the Route Processor (RP).

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs because the packet count is incremented for both the PXF engine and the RP.

- CSCse97843

  Symptoms: Input statistics for a serial interface that is part of an MLP bundle that is configured for LFI may be inaccurate (that is, the statistics may be too high).

  Conditions: This symptom is observed on a Cisco 10000 series after the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command is entered on the multilink interface at the far end. The symptom occurs because the "seq_num" is not reset to zero after the multilink interface at the far end is shut down and brought up again.

Workaround: There is no workaround.

- CSCsh05419

  Symptoms: When you paste a large configuration for a channelized port adapter, the standby RP may crash.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for HA.

  Workaround: Copy the configuration for the channelized port adapter to the startup configuration and then reload the router.

  Alternate Workaround: Do not copy the configuration. Rather, enter the configuration manually.

- CSCsh15664

  Symptoms: The PXF engine may crash, and the following error message may be generated:

  ```
  C10KEVENTMGR-1-MAJOR_FAULT PXF DMA TBB Length Error
  ```

  Conditions: This symptom is observed on a Cisco 10000 series sometime after you have changed the FRF.12 configuration.

  Workaround: The following procedures reduce the likelihood of the symptom occurring:

  1. Before you perform any modifications to FRF.12 configurations and the corresponding service policy, disable fragmentation.
  2. When you make modifications to the service policy, first detach the service policy, and then re-attach the modified service policy.

  For example, consider the following configuration:

  ```
  class-map match-any dscp_EF
     match ip dscp ef
   class-map match-any dscp_EF_ipprec_5
     match ip dscp cs5  ef
   class-map match-any dscp_AF4x
     match ip dscp cs4  af41  af42  af43
   class-map match-any dscp_AF3x
     match ip dscp cs3  af31  af32  af33
   !
   policy-map FRFRAG_child_A
     class dscp_EF
       priority
       police percent 50 25 ms 0 ms conform-action transmit exceed-action
  transmit violate-action
  drop
     class dscp_AF4x
      bandwidth percent 30
       random-detect dscp-based
       random-detect dscp 32 11 33 1
       random-detect dscp 34 11 33 1
       random-detect dscp 36 4 11 1
       random-detect dscp 38 4 11 1
     class dscp_AF3x
      bandwidth remaining percent 16
       random-detect dscp-based
  ```

```
    random-detect dscp 18 11 33 1
    random-detect dscp 20 4 11 1
    random-detect dscp 22 4 11 1
    random-detect 11 33 1
  class class-default
   bandwidth remaining percent 4
    random-detect dscp-based
!
policy-map FRFRAG_A
  class class-default
    shape 128
   service-policy FRFRAG_child_A
!
map-class frame-relay FRFRAG
 no frame-relay adaptive-shaping
 service-policy output FRFRAG_A
 frame-relay fragment 80
```

To modify this configuration, start by defining a new policy with the intended result:

```
#configure terminal
 Enter configuration commands, one per line.  End with CNTL/Z.
 (config)# policy-map FRFRAG_child_B
 (config-pmap)#   class dscp_EF_ipprec_5
 (config-pmap-c)#     priority
 (config-pmap-c)#police percent 50 25 ms 0 ms conform-action transmit
  exceed-action transmit
violate-action drop
 (config-pmap-c)#   class dscp_AF4x
 (config-pmap-c)#    bandwidth percent 30
 (config-pmap-c)#     random-detect dscp-based
 (config-pmap-c)#     random-detect dscp 32 16 40 1
 (config-pmap-c)#     random-detect dscp 34 16 40 1
 (config-pmap-c)#     random-detect dscp 36 6 16 1
 (config-pmap-c)#     random-detect dscp 38 6 16 1
 (config-pmap-c)#   class dscp_AF3x
 (config-pmap-c)#    bandwidth remaining percent 16
 (config-pmap-c)#     random-detect dscp-based
 (config-pmap-c)#     random-detect dscp 18 16 40 1
 (config-pmap-c)#     random-detect dscp 20 6 16 1
 (config-pmap-c)#     random-detect dscp 22 6 16 1
 (config-pmap-c)#     random-detect 16 40 1
 (config-pmap-c)#   class class-default
 (config-pmap-c)#    bandwidth remaining percent 4
 (config-pmap-c)#     random-detect dscp-based
 (config-pmap-c)#
 (config-pmap-c)# policy-map FRFRAG_B
 (config-pmap)#   class class-default
 (config-pmap-c)#     shape 256
 (config-pmap-c)#     service-policy FRFRAG_child_B
 (config-pmap-c)# exit
 (config-pmap)# exit
 (config)#
```

Then, remove the **fragment** keyword from the map class:

```
(config)# map-class frame-relay FRFRAG
 (config-map-class)#  no frame-relay fragment 80
 (config-map-class)# end
```

To allow time for the RP to process the configuration change, wait approximately 2 minutes. Then, remove the old service policy and apply the new one:

```
#configure terminal
 Enter configuration commands, one per line.  End with CNTL/Z.
 (config)# map-class frame-relay FRFRAG
 (config-map-class)#  no service-policy output FRFRAG_A
 (config-map-class)#  service-policy output FRFRAG_B
 (config-map-class)# end
```

Wait approximately 2 minutes, and then re-apply the **fragment** keyword to the map class:

```
#configure terminal
 Enter configuration commands, one per line.  End with CNTL/Z.
 (config)# map-class frame-relay FRFRAG
 (config-map-class)# frame-relay fragment 80
 (config-map-class)# end
```

Further Problem Description: Note that caveat CSCeh48541 is not related to this caveat because there are no “Priority Pak Q” drops on the interfaces.

- CSCsi31041

  Symptoms: When the **service local** command is configured under a policy map, service is denied.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG and that is configured for AAA.

  Workaround: There is no workaround.

- CSCsi67246

  Symptoms: A compact flash card in a router may not be accessible from the Cisco IOS prompt or from the ROMmon prompt. When you attempt to access the flash card from the Cisco IOS prompt, the following error message is generated:

  ```
  %Error opening disk0:/ (No device available)
  ```

  From the ROMmon prompt, any attempt to access the compact flash card to boot the image fails.

  Conditions: This symptom is observed on a Cisco 7304 that has a compact flash card from a particular this-party vendor. The compact flash card has a date code is earlier than “060728” (that is, 7/28/06) and a vendor part number that starts with “CCF”.

  Workaround: There is no workaround.

- CSCsi70224

  Symptoms: After a switchover occurs on a Cisco 10000 series, the boot variable may not be present on the standby PRE, which can be seen in the output of the **show bootvar** EXEC command.

Conditions: This symptom is observed when the following events occur:

1. You ensure that the BOOT variable is present in the startup configuration.
2. You enter the **no boot system** global configuration command.
3. You enter the **redundancy force-failover main-cpu** EXEC command on the active PRE and do not save the configuration.

In this situation, when the new standby PRE comes up and after the bulk synchronization has occurred, the BOOT variable is not present. If another switchover occurs, the BOOT variable is not present on the new active PRE nor the new standby PRE.

Workaround: Ensure that the **boot system** global configuration command is present in the running configuration.

- CSCsj14584

  Symptoms: A Cisco 7304 with an NSE-150 may not be stable in a configuration with 1000 MVPNs and may crash after all protocols (BGP, OSPF, PIM and IGMP), have started.

  Conditions: This symptom is observed when there is a large number of OSPF routes and occurs because the router runs out of I/O memory. OSPF uses I/O memory to allocate a database summary. Therefore, with a large umber of OSPF routes, more I/O memory is required.

  Workaround: Increase the size of the I/O memory.

- CSCsj26971

  Symptoms: A Cisco 10000 series may generate the following error message:

  ```
  %HQF_MAP_TT-3-HQF: hmt_get_new_class_blt_index error detected: Failed to allocate new
  class blt.
  ```

  Conditions: This symptom is observed on a Cisco 1000 series that has a PRE-3 after sessions that have queueing policy maps attached have been churned more than 1 million times.

  Workaround: There is no workaround.

- CSCsj51087

  Symptoms: Poor throughput may occur when MLP and QoS are configured, and 10 percent of the traffic may be lost.

  Conditions: This symptom is observed on a Cisco 10000 series when a priority queue is configured and when traffic is queued only in non-priority queues. The symptom occurs only with certain QoS policies and packet sizes.

  Workaround: There is no workaround. Note that the symptom is unlikely to occur in a production network.

- CSCsj52561

  Symptoms: After an interface has flapped, packets may be dropped, and a “FIB RPF fail” error message may be generated for the PXF engine. This situation affects asymmetric routing.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Configure Reverse Path Forwarding (RPF) on the interface and then remove it again, as in the following example. Doing so restores the original interface flags on the PXF engine.

  ```
  int atm 1/0/0.100
  ip unicast reverse-path
  no ip unicast reverse-path
  ```

- CSCsj57953

  Symptoms: A Cisco 7304 may hang and may not generate any keepalives or route updates.

Conditions: This symptom is observed only on a Cisco 7304 that has an NSE-150.

Workaround: Call Cisco TAC for assistance with a workaround.

Further Problem Description: The root cause of the symptom is a lock-up in the transmission of packets from the RP to the PXF engine. The packets are not completely read from an internal memory. This situation eventually blocks the transmission of later packets from the RP to the PXF engine.

- CSCsj78315

  Symptoms: After a PRE switchover has occurred, a PVC may hang. When the **oam-pvc manage** command is configured, the PVC in the down state; when the **oam-pvc manage** command is not configured, the PVC appears to be up but no traffic passes through the PVC.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for SSO.

  Workaround: Delete and re-define the PVC to recover from the symptoms.

- CSCsj80375

  Symptoms: A T3/E3 serial SPA may not come up because the line protocol remains down, and the output of the **show controllers serial** command does not generate any output for the T3/E3 serial SPA.

  Conditions: This symptom is observed on a Cisco 7304 when you apply the configuration for the first time after the router has booted.

  Workaround: Unconfigure and reconfigure the **card type** command for the T3/E3 serial SPA.

Wide-Area Networking

- CSCsd11874

  Symptoms: When you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an MFR interface when the bundle links are down, the serial interfaces that are associated with the MFR interface remain in the IDLE state.

  Conditions: This symptom is observed on a Cisco router that is configure for MFR.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on each serial interface that is associated with the MFR interface.

- CSCsi78968

  Symptoms: When a a multilink bundle comes up, the following error message may be generated:

  ```
  SYS-2-INTSCHED: ‘idle’ at level 2 -Process= "PPP Events"
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(31)SB6

Cisco IOS Release 12.2(31)SB6 is a rebuild release for Cisco IOS Release 12.2(31)SB2. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB6 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsf96138

  Symptoms: The MIB object value of "Number of Octets in use" (rttMonCtrlOperOctetsInUse) is always set to zero.

  Conditions: This symptom is observed on a Cisco router that has an Echo probe configured.

  Workaround: There is no workaround.

- CSCsh71307

  Symptoms: A router may crash when you enter the **show cdp entry** *device-name* command.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G2 and a Port Adapter Jacket Card in which a PA-2CT3 port adapter is installed.

  Workaround: There is no workaround.

- CSCsi13207

  Symptoms: The output of the **show ip cache flow** command for NetFlow on an LNS shows the physical ingress interface as the source interface for packet flows instead of the virtual-access interface.

  Conditions: This symptom is observed on a Cisco 7206VXR that runs Cisco IOS Release 12.2(28)SB3 and that functions as an LNS when the following configuration is present:

  – The physical ingress interface that faces the LAC is "fas0/0" and has the **ip flow ingress** command enabled.

  – The **flow-sampler one-in-hundred** command is enabled on the virtual-template interface.

  Workaround: Do not enter the **ip flow ingress** command on the physical ingress interface. Rather, enter the **ip flow ingress** command on the virtual-template interface, bring down the tunnel, and then bring up the tunnel.

- CSCsi28884

  Symptoms: The attribute list may not be downloaded for a particular service.

  Conditions: This symptom is observed on a Cisco platform that is configured for AAA when local authorization is configured and when the attribute list is downloaded. The following shows a configuration in which the symptom occurs:

  ```
  policy-map type service abcd
   aaa attribute list cisco
   service local
  
  aaa attribute list cisco
   attribute type addr-pool "cisco" protocol ip
   attribute type ppp-author-list "cisco"
   attribute type ppp-authen-list "cisco"
  ```

  Workaround: Ensure that the same name is used for the *policy-map-name* argument of the **policy-map type service** *policy-map-name* command (abcd in the example above) and the *list-name* argument of the **aaa attribute list** *list-name* command (cisco in the example above).

- CSCsi80159

  Symptoms: A Cisco router that functions as an ISG may not send RADIUS attribute 44 in the RADIUS Access Request when the **vrf default** keywords are present in the command line, as in the following example:

  ```
  radius-server attribute 44 include-in-access-req vrf default
  ```

  This situation affects the prepaid billing service for ISG-based customers because the billing system cannot re-authorize a subscriber after its quota runs out. The billing system is not able to consolidate the AAA accounting sessions without RADIUS attribute 44 in the RADIUS Access Request for re-authorization. Even if the ISG prepaid threshold is zero, re-authorization fails because the service quota is exhausted, but subscriber's session remains active.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB or one of its rebuilds because in these releases the **vrf default** keywords are added by default.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCea90941

  Symptoms: The EIGRP Stub Routing feature may be missing from the configuration.

  Conditions: This symptom is observed when a Cisco router on which the EIGRP Stub Routing feature is enabled is reloaded, or when the Enhanced Interior Gateway Routing Protocol (EIGRP) process is restarted.

  Workaround: There is no workaround. Re-enable the EIGRP Stub Routing feature.

- CSCek43230

  Symptoms: The CPU usage of the RP may be very high on a router that is configured for eiBGP Multipath Load Sharing.

  Conditions: This symptom is observed on a Cisco router that advertises a few prefixes that are loadbalanced.

  Workaround: There is no workaround.

- 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.

- CSCin95836

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

This advisory is posted at

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

- 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.

- CSCsg07742

  Symptoms: The attributes that are configured in a site map may not automatically be applied to the BGP table when the associated interface is running other routing protocols such as RIP or OSPF.

  Conditions: This symptom is observed on a Cisco router when routes are redistributed into BGP.

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

- 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.

- 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.

Miscellaneous

- 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 nor release-specific.

Workaround: Do not query the entire ciscoCBQosMIB and do not poll the cbQosQueueingStatsTable or cbQosPoliceStatsTable.

- CSCek53660

  Symptoms: A Cisco 10000 series that has a PRE-3 may reload unexpectedly when PPPoA calls are brought up aggressively.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB during a test in which sessions are brought up and down by emulating client power outages, forcing OIRs, and switchovers.

  Workaround: There is no workaround.

- CSCek65491

  Symptoms: A router that is configured for HA may unexpectedly reload because of a spurious memory access.

  Conditions: This symptom is observed on a Cisco 10000 series when an L2TP tunnel interface flaps, causing a spurious memory access in the chunk memory. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

  Further Problem Description: Note that SSO is not supported on a Cisco 10000 series that runs Cisco IOS Release 12.2(28)SB or one of its rebuilds and that is configured for broadband aggregation:

  "In Cisco IOS Release 12.2(28)SB, the Cisco 10000 series supports Route Processor Redundancy Plus (RPR+), and Stateful Switchover (SSO). However for broadband aggregation features, the Cisco 10000 series supports RPR+ only."

  For more information, see the Broadband Aggregation and Leased-Line Overview document:

  http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_gu ide_chapter09186a00805057de.html

- 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. However, the symptom is not platform- nor release-specific.

  Workaround: There is no workaround.

- CSCek68047

  Symptoms: Authentication may be skipped during account logon.

  Conditions: This symptom is observed when an IP session is brought up with a default service before account logon.

Workaround: Do not configure a default service before account logon.

- CSCek71805

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

  1. Symptom 1: A PA-8B-ST port adapter may be powered down when you boot the router.

     Condition 1: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G2 and a PA-8B-ST port adapter. The symptom does not occur with an NPE-G1.

     Workaround 1: Perform a software OIR to bring up the port adapter.

  2. Symptom 2: The ISDN layers may not come up.

     Condition 2: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G2 and a PA-8B-ST port adapter. The symptom does not occur with an NPE-G1.

     Workaround 2: Enter the **debug bri-interface** command to bring up the ISDN layers.

- CSCek74740

  Symptoms: Shaping and random detect may not be enabled when you attempt to do so.

  Conditions: This symptom is observed on the fourth native Gigabit Ethernet port on a Cisco 7201 that runs Cisco IOS Release 12.2SB but may not be platform- and release-specific.

  Workaround: There is no workaround.

- CSCek75633

  Symptoms: A router may crash when you attach a VC class to an ATM bundle.

  Conditions: This symptom is observed on a Cisco 7200 series but is platform-independent.

  Workaround: There is no workaround.

- CSCse64269

  Symptoms: When an IMA group interface is configured on a Cisco 7600 series, the output of the **show ip interface brief** command may show the line protocol of member link as down when it is not down.

  Conditions: This symptom is observed when the Cisco 7600 series has an IMA group interface configured on a PA-A3-8T1IMA or PA-A3-8E1IMA port adapter. The symptom is not platform-specific.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the member link of the IMA group on the PA-A3-8T1IMA or PA-A3-8E1IMA port adapter.

- CSCsg03483

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

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

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

  Workaround: There is no workaround.

- 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.

- CSCsg56947

  Symptoms: When you perform and OIR of a SPA-2XOC3-POS, the HC counters may stop functioning.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S10 or a later release or Release 12.2(28)SB5.

  Workaround: Do not perform an OIR. Rather, reload the SPA when there is an opportunity.

- CSCsg77139

  Symptoms: After you have reloaded a router, VRF routes disappear.

  Conditions: This symptom is observed when you reload a router the processes a heavy traffic flow.

  Workaround: Enter the **clear ip route vrf** *vrf-name* command.

  Alternate Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface from which the VRF routes have disappeared.

- 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 may be platform-independent.

  Workaround: There is no workaround.

- CSCsg99958

  Symptoms: Queue and buffer leaks may occur, and the output of the **show pxf cpu queue summary** command may show that many queues are being recycled.

  Conditions: This symptom is observed on a Cisco 10000 series that has a class queue configured for a UDP port and occurs after a large number of serial interfaces flap on the router at the far-end.

  Workaround: Add a queue-limit for the class queue on the UDP port, as in the following example:

```
policy-map IPBH
  class udp_traffic
    police percent 90 17 ms 17 ms conform-action transmit exceed-action drop
violate-action drop
 priority
queue-limit 512
  class tcp_traffic
    bandwidth percent 9
    queue-limit 256
  class class-default
    bandwidth percent 1
    queue-limit 128
```

- 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.

- CSCsh59270

  Symptoms: When L4 redirect is configured for a session or traffic class, the downstream packet counters may be double counted in the output of the **show pxf cpu isg interface** *virtual access* command.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG.

  Workaround: There is no workaround.

- CSCsh82884

  Symptoms: High PQ latency may occur with a large number of PPPoEoX sessions in a LAC/LNS topology when policy maps are applied to sessions either via a virtual template or via RADIUS AVPs.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur for the same PPPoEoX QoS configuration in a PTA environment.

- CSCsh93030

  Symptoms: When a VLAN group policy is attached to a Gigabit Ethernet main interface, queues are allocated properly on the interface. However, after you have entered the **microcode reload pxf** command, or after a PXF crash has occurred, the queues are no longer properly allocated.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, remove and re-attach the VLAN group policy to the Gigabit Ethernet main interface.

- CSCsh94637

  Symptoms: An NPE-G1 may crashes because of a bus error and generate the following error message:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address TLB (store) exception, CPU signal 10,
  PC = 0x61F1D0D0
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(31)SB2 and that is configured for L2TP. The symptom may not be platform-specific.

  Workaround: There is no workaround.

- CSCsi15304

  Symptoms: A router may crash when you remove a PBR configuration from a virtual access interface.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Do not configure PBR on an interface that is used for user sessions.

- CSCsi15995

  Symptoms: Multilink interfaces stop transmitting traffic after a PRE failover has occurred.

Conditions: This symptom is observed on a Cisco 10000 series that has two OC-12 ports that function as active ports in an APS configuration and that are configured with multiple multilink interfaces.

Workaround: Enter the **microcode reload pxf** command. Note that entering the **hw-module subslot** *slot/subslot* **reset** command for the affected ports does not resolve the symptom.

- CSCsi22585

  Symptoms: DNS requests from a PC client may time out.

  Conditions: This symptom is observed on a cisco router that functions as an ISG, that is located between a PC and a DNS server, and that redirect DNS requests to a local DNS server.

  Workaround: There is no workaround.

- CSCsi25871

  Symptoms: A Cisco 10000 series may show the wrong traffic class statistics for a session when traffic class services with priorities are applied dynamically to the session.

  Conditions: This symptom is observed only when traffic class services are downloaded that have higher priorities than the priorities that are already loaded onto the session.

  Workaround: There is no workaround.

- CSCsi25886

  Symptoms: The output of the **show policy-map interface** command and **show policy-map session** command shows all policing counters as zero for policies that are applied to LNS sessions.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs only with LNS sessions. The symptom does not occur with LAC or PTA sessions.

  Workaround: There is no workaround.

- CSCsi45831

  Symptoms: There may be a delay in the creation of IP sessions over an interface that is configured for QinQ support.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when the **initiator dhcp class-aware** command is enabled to place the clients in a specific VRF.

  Workaround: There is no workaround.

- CSCsi49907

  Symptoms: A memory leak may cause a slow response and time-outs during the set-up of new IP sessions, and the connection speed for established sessions may be very slow. To verify that there is a memory leak, enter the **show memory debug leak summary** command, and look for “Alloc PC” in the output.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB3 and that has the following configuration commands under a BVI or on an IP interface:

  ```
  service-policy type control XXXX
   ip subscriber routed
    initiator dhcp class-aware
  ```

  Workaround: There is no workaround.

- CSCsi52268

  Symptoms: A router may run out of memory when you scale sessions with QoS and distribute them among a large number of subinterfaces.

Conditions: This symptom is observed on a Cisco router such as a Cisco 10000 series with a PRE3 that is configured for Hierarchal Queuing Framework (HQF). The symptom is not platform-specific. The symptom occurs when the following conditions are present:

- Sessions are being scaled.
- Per-session shaping and/or queuing is configured.
- The number of sessions per subinterface is small.
- hierarchical queuing policy maps on sessions with aggregate shaping is configured, meaning that the subinterfaces are shaped as well. The subinterfaces are either shaped VLAN-QinQ subinterfaces or shaped ATM VC subinterfaces.

Workaround: There is no workaround.

- CSCsi52839

  Symptoms: The PXF engine of a Cisco 10000 series may crash and the following error message may be generated:

  ```
  %C10KEVENTMGR-1-MAJOR_FAULT: PXF DMA FTC Move Command with Continue Error PXF DMA
  Error - Input Command Has Sequence Problem, Restarting PXF in an LNS config.
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3 and that runs Cisco IOS Release 12.2(31)SB3b and that processes L2TP traffic.

  Workaround: There is no workaround.

- CSCsi53469

  Symptoms: A router may hang for approximately 7 minutes.

  Conditions: This symptom is observed when you attempt to configure the **range pvc** command in a manner that exceeds the interface limit.

  Workaround: There is no workaround.

- CSCsi57031

  Symptoms: On a pseudowire that is configured on an OC-12 ATM interface, when you delete the **oam-ac emulation-enable** command, enter the **write memory** command, and then initiate an SSO switchover, the new standby PRE continues to reboot because of a configuration mismatch with the new active PRE.

  Conditions: This symptom is observed on a Cisco 10000 series when the new active PRE has the **oam-ac emulation-enable** command in its configuration but the new standby PRE does not, causing a configuration mismatch. The symptom may not be platform-specific.

  Workaround: Reload the new active PRE, then remove the **oam-pvc manage 0** command from its configuration.

- CSCsi57207

  Symptoms: A bus error crash is seen on a Cisco router that is running Cisco IOS Release 12.2(31)SB3.

  Conditions: This symptom is seen when PPPoE/PPPoA is configured with PPP “idletimeout” and PPP keepalive.

  Workaround: There is no workaround.

- CSCsi57924

  Symptoms: AToM Xconnect end-to-end connectivity may be lost when MAC Address Accounting is configured on the Xconnect circuit.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 or an NSE-150.

Workaround: There is no workaround.

- CSCsi60004

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

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

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

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

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

- CSCsi73899

  Symptoms: A Cisco 7301 or Cisco 7304 that is configured to use MPLS service policies on some interfaces may crash. The crash may be preceded by following error messages:

  ```
  %SYS-2-CHUNKBOUNDSIB: Error noticed in the sibling of the chunk pak subblock c, Chunk
  index : 25, Chunk real max :25
  ```

  and

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 45FE855C data 45FE862C
  chunkmagic 15A3C78B chunk_freemagic 1000000
  ```

  Conditions: This symptom is observed on a Cisco 7301 and Cisco 7304 that run Cisco IOS Release 12.2(31)SB and is not related to a specific command sequence. However, note that the crash is platform-independent. For example, the crash could also occur on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCsi75638

  Symptoms: When QoS is applied to PPPoEoA sessions, police statistic counters may remain zero.

  Conditions: This symptom is observed only on a Cisco 10000 series that has a PRE-3 and that runs Cisco IOS Release 12.2(31)SB5. The symptom does not occur in Cisco IOS Release 12.2(31)SB3.

  Workaround: There is no workaround.

- CSCsi76569

  Symptoms: A Cisco 7200 series may crash during bootup or while writing or erasing the configuration during the “flow_def_master_list_lookup” process.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 or NPE-G2. The symptom occurs during bootup or when a configuration is written to or erased from memory. The symptom may also occur when you enter the **show running-config** command.

  Workaround: There is no workaround.

- CSCsi78785

  Symptoms: A router may crash when a policy map is unconfigured.

  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.

- CSCsi91674

  Symptoms: A PPP over Layer 2 Tunneling Protocol (PPPoL2TP) session may fail to establish itself.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3, that functions as an LNS, and that terminates PPPoL2TP tunnels.

  Workaround: There is no workaround.

- CSCsi93020

  Symptoms: A router may crash when it functions as a LAC with a single PPPoE session that is locally terminated and when a service policy contains CoS marking or any other non-supported configuration.

  Conditions: This symptom is observed under the following conditions:

  1. Attach the policy to both the outbound and inbound interfaces of the virtual template.
  2. Unconfigure the policy from the outbound and inbound interfaces of the virtual template.
  3. Re-attach the policy to the outbound interface of the virtual template.

  Workaround: There is no workaround.

- 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.

- CSCsi97545

  Symptoms: After a microcode reload, a policy may no longer be attached to an interface.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, remove the policy from the interface and then re-attach it.

- CSCsi98341

  Symptoms: There rate of collisions and deferred packets may increase.

  Conditions: This symptom is observed on a Cisco 10000 series because the Inter Packet Gap (IPG) and Inter Frame Spacing1 (IFS1) in the PRE-2 MAC register CSR125 are not set correctly.

  Workaround: There is no workaround.

- CSCsj04527

  Symptoms: The standby RP may enter ROMmon when the router functions in RPR+ mode.

  Conditions: This symptom is observed on a Cisco 10000 series that has a 6CHT3-1 line card when you unconfigure and re-configure a Frame Relay interface under RPR+ mode.

  Workaround: Do not configure RPR+. Rather, configure SSO.

- CSCsj07446

  Symptoms: When L4 Redirect is configured for a traffic class with an inbound ACL only, downstream traffic may not be translated.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG.

  Workaround: Configure both an inbound and outbound ACL for the traffic class.

- CSCsj07886

  Symptoms: After a switchover has occurred, the standby PRE may reboot continuously.

  Symptoms: This symptom is observed on a Cisco 10000 series when you enable and then disable the **oam-ac emulation-enable** command, causing a configuration mismatch between the active and standby PREs.

  Workaround: There is no workaround.

- CSCsj17185

  Symptoms: MLP and serial interfaces may bounce, and the following error messages may be generated:

  ```
  %C10K_QUEUE_CFG_WARNING-2-EREVENT: Warning @ Bundle FIFO will not drain:5353
  -Process= "PPP Events", ipl= 0, pid= 268 %C10K_MULTILINK_USER_WARNING-2-CRITEVENT:
  Cannot install mlp link Serial5/0/0/2:1
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that has an MLP interface to which a service policy is attached and occurs after you have performed the following events:

  1. You remove the global policy map and re-add the policy map.
  2. You add the service policy back to the MLP interface.
  3. You enter the **shutdown** interface configuration command quickly followed by the **no shutdown** interface configuration command on the MLP interface.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, remove and re-add the MLP interface.

- CSCsj19536

  Symptoms: When the Prepaid Volume Monitor is configured to monitor PPPoX and IP sessions, reauthorizations do not occur at the required threshold expiration, and quota counts are incorrect. However, time is monitored as expected.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB6 and that functions as an ISG.

  Workaround: There is no workaround.

- CSCsj21333

  Symptoms: The standby PRE may reload continuously after the active PRE has crashed because of a watchdog timeout. When this situation occurs, the active PRE generates the following error message:

  ```
  GET_PEER_BUFFER: Get message buffer failed.
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB.

  Workaround: There is no workaround. When the symptom has occurred, you must reset both PREs.

- CSCsj25562

  Symptoms: A router that functions in a BBA QoS configuration may crash when a shaper policy map is removed from a PPPoEoVLAN subinterface while QoS sessions are being established.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3 but may not be limited to a PRE-3.

  Workaround: There is no workaround.

- CSCsj29687

  Symptoms: An ATM VC may remain down until you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface on which the ATM VC is configured.

  Conditions: This symptom is observed after a service policy has been added to or deleted from the ATM VC.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the ATM VC after the service policy has been added deleted.

- CSCsj30138

  Symptoms: The standby PRE-2 may fail to boot. It may reach the standby hot state but may then reload after a "Bulk-sync failure" error is displayed on the console:

  ```
  Config Sync: Bulk-sync failure due to BEM mismatch
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB5 when SSH Version 1 (SSHv1) or SSH Version 2 (SSHv2) is configured. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCsj39272

  Symptoms: All VCs that are configured on an ATM main interface may remain down until the ATM line card is reloaded.

Conditions: This symptom is observed on a Cisco 10000 series that has an ATM main interface that is administratively down when first a PRE switchover occurs and then you enter the **no shutdown** interface configuration command on the ATM main interface. The symptom may not be platform-specific.

Workaround: There is no workaround.

- CSCsj40492

  Symptoms: A router may crash when you enter the **no card** command to remove the configuration of a line card.

  Conditions: This symptom is observed on a Cisco 10000 series after you have removed a line card with the intention of replacing it with a line card of another type.

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCee32814

  Symptoms: TCP source ports that are used for connections that originate from a Cisco IOS platform may be chosen in a predictable manner.

  Conditions: This symptom is observed for outbound TCP connections for which a particular source port is not required.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCek76406

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

  1. Symptom 1: A Cisco 7200 series may crash when payload compression is added to or removed from an MFR interface that has interface fragmentation configured.

     Condition 1: This symptom is observed when traffic is sent through MFR interface which has or had interface fragmentation and payload compression configured. The symptom may not be platform-specific.

     Workaround 1: There is no workaround. Do not configure both interface fragmentation and payload compression on an MFR interface.

  2. Symptom 2: A Cisco 7200 series may crash when you remove interface fragmentation from an interface that is configured for Frame Relay encapsulation while traffic is running.

     Condition 2: This symptom is observed with both serial Frame Relay and MFR interfaces. The symptom may not be platform-specific.

     Workaround 2: Shut down the interface before you remove interface fragmentation.

- CSCsi51530

  Symptoms: If non-Cisco PPPoA client is dialing into a Cisco router, the call may fail at the PPP authentication phase. When this situation occurs, the following error message is generated:

  ```
  Failed to send an authentication request x
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB5.

  Workaround: There is no workaround.

- CSCsi57143

  Symptoms: After an SSO switchover has occurred, some serial interfaces may remain down on the newly active RP.

  Conditions: This symptom is observed on a Cisco router that has several serial interfaces with PPP encapsulation up and running on the active RP before the SSO switchover occurs.

  Workaround: There is no workaround.

- CSCsi69009

  Symptoms: High CPU usage may occur when IPCP is being renegotiated. Eventually, the high CPU usage may cause buffers to be backed up, may cause error message to be generated, and may cause L2TP tunnels to be dropped.

  Conditions: This symptom is observed on a Cisco router when clients renegotiate IPCP unnecessarily. You can verify this situation by enabling the **debug ppp negotiation** command or by configuring RADIUS authorization and then checking the virtual-access interface for the phrase "cloned from: AAA, AAA, ..." (that is, multiple instances of AAA) as identification.

  Workaround: There is no workaround.

  Further Problem Description: You can alleviate the situation somewhat by configuring the NCP Timeout to 15 seconds to disconnect clients that take a long time to renegotiate IPCP. You can also do the following:

  - Increase the hello timers for L2TP and for the receive windows.
  - Configure the timers under the virtual template.
  - Do not configure the **redistribution connected** command under a routing protocol such as (but not limited to) EIGRP, RIP, or OSPF.
  - Ensure that the IP local pools are concise. For example, create one statement for multiple /24s instead of splitting all /24s on single lines, because with single lines, the look-up becomes long and contributes to the high CPU usage.

- 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.

- CSCsi94498

  Symptoms: Alternate packets may be dropped during a ping test.

  Conditions: This symptom is observed when you initiate a ping over a Frame Relay PVC bundle.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(31)SB5

Cisco IOS Release 12.2(31)SB5 is a rebuild release for Cisco IOS Release 12.2(31)SB2. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB5 but may be open in previous Cisco IOS releases.

Basic System Services

- 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.

Interfaces and Bridging

- CSCeh17935

  Symptoms: When you perform an Online Insertion and Removal (OIR) of an ATM port adapter, tracebacks are generated.

Conditions: This symptom is observed on a Cisco 7200 series when the ATM port adapter is up and has a VC configured, when traffic passes through the ATM interface of the port adapter during the OIR, and when the ATM interface of the port adapter is oversubscribed.

Workaround: There is no workaround.

- CSCsi19949

  Symptoms: An ATM interface goes down after you have reloaded a router.

  Conditions: This symptom is observed on a Cisco 7200 series that has a PA-A3-OC3MM port adapter but could also occur on other platforms that have an ATM port adapter.

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

- 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

- CSCeg52659

  Symptoms: A Cisco 7200 series may not withdraw a BGP route from an iBGP peer.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(3) when the **clear ip bgp** *neighbor-address* **soft out** command is entered for one of the members of the peer group of which the Cisco 7200 series is a member and when some changes to the outbound policy are made to the same member of the peer group. This situation causes some prefixes to remain struck in the other members of the peer group. The symptom may also occur in other releases.

  The symptom is a very old behavior of the BGP peer group functionality: when one member of a peer group is cleared via either a hard reset or a soft reset and a policy change causes some of the prefixes to be withdrawn, inconsistencies may occur in the routes on the other members of the peer group.

  Workaround: For peer groups and neighbors that are members of a peer group, do not enter the BGP neighbor-specific **clear ip bgp** *neighbor-address* **soft out** command or the **clear ip bgp** *neighbor-address* command. Rather, enter the peer group-specific **clear ip bgp** *peer-group-name* **soft out** command or the **clear ip bgp** *peer-group-name* command.

- 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.

- CSCsg45637

  Symptoms: A traceback may be generated when the router accesses the “bgp_vpnv4_lookup_prefix” function.

  Conditions: This symptom is observed on a Cisco router that is configured for BGP VPNv4.

  Workaround: There is no workaround.

- 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.

- 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.

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.

- CSCek52651

  Symptoms: The drop rate counters for an interface may show an incorrect value of 19 characters.

  Conditions: This symptom is observed when you apply a service policy with traffic shaping to an interface.

  Workaround: There is no workaround.

- CSCek57267

  Symptoms: CPUHOG and IPCOIR errors may occur on a Cisco router when you change the IP address of a loopback interface that is associated with a large number of active PPP sessions.

Conditions: This symptom is observed on a Cisco 10000 series that runs slowly when interfaces flap. The symptom is platform-independent.

Workaround: There is no workaround.

- CSCek57932

  Cisco uBR10012 series devices automatically enable Simple Network Management Protocol (SNMP) read/write access to the device if configured for linecard redundancy. This can be exploited by an attacker to gain complete control of the device. Only Cisco uBR10012 series devices that are configured for linecard redundancy are affected.

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

  This advisory is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20080924-ubr.shtml.

- CSCek72665

  Symptoms: Tracebacks may be logged in the console log of the standby PRE.

  Conditions: This symptom is observed on a Cisco 10000 series when a T1 channel group is configured on a T3 controller of 6-port channelized T3 line card.

  Workaround: Reset the standby PRE.

- CSCin99249

  Symptoms: A Cisco 7200 series that is configured with a Port Adapter Jacket Card (C7200-JC-PA) may crash after you have performed a soft OIR of the port adapter that is installed in the Port Adapter Jacket Card.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 when you perform the following steps:

  1. First, you perform a soft OIR by entering the **hw-module slot 7** command with either the **stop** or **start** keyword for the port adapter that is installed in the Port Adapter Jacket Card.
  2. Then, you either enter the **reload** command or the **show ip interface brief** command.

  The symptom does occurs only when the not occur on a Cisco 7200 series that has an NPE-G2.

  Workaround: There is no workaround.

  Further Problem Description: For this caveat, while the Port Adapter Jacket Card slot address is slot 0 of the router chassis, note that the port adapter in the Port Adapter Jacket Card is identified as residing in port adapter slot 7.

- CSCin99725

  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
```

- 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.

- 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.

- 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.

- CSCse12154

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

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

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

- CSCse24889

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

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

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

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

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

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

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

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

  Further Problem Description:

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

  http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_chapter09186a0080716ec2.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

- CSCse55371

  Symptoms: A policing error may occur on a DHCP IP session when local authorization is configured.

Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG).

Workaround: Configure a DHCP IP session and RADIUS authorization.

- 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.

- 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.

- CSCsg10134

  Symptoms: A router crashes when PPPoEoA sessions are torn down.

  Conditions: This symptom is observed when the maximum number of class-map instances are configured on the router.

  Workaround: There is no workaround.

- 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.

- CSCsg98611

  Symptoms: When you enter the **issu loadversion** command, the ISSU mail fail with the following error message:

  ```
  Active [ ] and Standby [ ] images should be the same for running loadversion
  ```

  Conditions: This symptom is observed in a rare situation on a Cisco router and occurs even when the Cisco IOS software images on the active and standby RPs are identical.

  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.

- 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.

- CSCsh23312

  Symptoms: A Cisco 10000 series may drop MPLS packets from an ingress interface.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(28)SB or a later release after an FSU has occurred on a neighboring router.

  Workaround: Enter the **microcode reload pxf** command on the Cisco 10000 series.

- CSCsh47740

  Symptoms: In an ATM pseudowire configuration, when you reset a line card by entering the **hw-module slot** *slot-number* **reset** command, the pseudowire comes back up but the traffic does not resume, and an end-to-end ping fails.

  Conditions: This symptom is observed on a Cisco 10000 series.

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

- CSCsh54999

  Symptoms: A router may crash when the dynamic ACL timer expires.

  Conditions: This symptom is observed on a Cisco router only when the **show access-list** command is entered before the timer expires.

  Workaround: There is no workaround.

- CSCsh57611

  Symptoms: Frame Relay end-to-end keepalives may unexpectedly time out.

  Conditions: This symptom is observed on a Cisco 7206VXR that has an NPE-G1 and that runs Cisco IOS Release 12.2(31)SB2.

Workaround: There is no workaround.

- CSCsh61595

  Symptoms: Some serial interfaces continuously flap and do not remain in the up state because a PPP negotiation loop occurs.

  Conditions: This symptom is observed on a Cisco 10000 series after a large number of interfaces has flapped from more than two hours.

  Workaround: There is no workaround.

- CSCsh64559

  Symptoms: A multicast ping may be dropped by a Cisco 7304.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 or NSE-150 when the router attempts to respond to the ping. The symptom does not occur for traffic that traverses the router.

  Workaround: There is no workaround.

- CSCsh64709

  Symptoms: A Cisco 7304 may stop passing traffic through its Gigabit Ethernet interfaces. Even though a **show** command shows that the interfaces continue to be in the up/up state and respond to removal of the network cable, no traffic is transmitted from the interfaces. The CPU usage of the PXF engine may reach 100 percent, or at least higher than you would reasonably expect.

  Conditions: This symptom is observed on a Cisco 7304 with an NSE-100 or NSE-150 when there are input and output ACLs configured and when ACL output deny drops occurs. In this situation, the PXF engine attempts to generate ICMP unreachables, some of which are looping continuously in the PXF engine, causing the CPU usage of the PXF engine to be high.

  Workaround: Disable ICMP unreachables on the interfaces by entering the **no ip unreachable** command. Doing so prevents the CPU usage of the PXF engine from becoming higher but does not decrease its current level. To enable the CPU usage of the PXF engine to return to a normal level, reload the router after you have disabled ICMP unreachables on the interfaces.

- CSCsh68285

  Symptoms: A Cisco 10000 series may generate a traceback when you attempt to create a duplicate IP session.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an Intelligent Service Gateway (ISG) and occurs only with IP sessions that are connected via Layer 2. The symptom occurs because of a timing issue.

  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.

- CSCsh91659

  Symptoms: When a SmartJack is configured in a loopback, the PRE in slot B of a Cisco 10000 series may crash continuously because bulk synchronization fails between the PREs.

Conditions: This symptom is observed when you enter the **t1** *t1-number* **loopback remote line inband maintenance** command.

Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, remove all occurrences of the **t1** *t1-number* **loopback remote line inband maintenance** command from the running configuration via the console of the active PRE.

- CSCsh91746

  Symptoms: After creating T1 links on a channelized STM-1 interface, you cannot access the associated interfaces in global configuration mode or Exec mode.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Creating a new interface may clear the condition. If it does not, reload the router.

- CSCsh92854

  Symptoms: When the **ip cef** command is enabled, output bytes of a virtual-access interface do not increment correctly.

  Conditions: This symptom is observed on a Cisco router that has a PPPoVPDN virtual-access interface when the VPDN traffic is sent over an ATM interface. The symptom does not occur when the VPDN traffic is sent over a Gigabit Ethernet interface.

  Workaround: If this is an option, disable CEF on the interface from which the VPDN traffic is switched. However, doing so may affect the performance of the platform. If this is not an option, there is no workaround.

- CSCsh93114

  Symptoms: The following symptoms may occur for prepaid accounting:

  - Prepaid service gigaword counters remain zero while gigaword attributes 52 and 53 are correct on the parent session. When you enable the **debug radius** command, gigaword attributes 52 and 53 are shown for the parent session:

    ```
    ...
    RADIUS(0000000D): Send Accounting-Request to 10.30.81.45:1813 id 21651/19, len
    391
    RADIUS:  authenticator 6C 91 FF EE 94 43 4A 76 - 8A FD 94 53 66 E3 53 25
    RADIUS:  Acct-Session-Id     [44]  18  "0A0A440200000003"
    ...
    RADIUS:  Acct-Input-Giga-Word[52]  6   1
    RADIUS:  Acct-Output-Giga-Wor[53]  6   0
    ```

  - The prepaid service always sends the rollover counters in “I” and “O” as zero although the definitions are “I<HC>;<LC>” and “O<HC>;<LC>” in which HC indicates the rollover counter and LC indicates the lower 32 bit of the input and output octets counters.

    ```
    ...
    (0000000D): Send Accounting-Request to 10.30.81.45:1813 id 21651/20, len 299
    RADIUS:  authenticator 0A C2 61 78 C9 63 04 64 - 6E C4 F4 B3 11 E9 DF A4
    RADIUS:  Acct-Session-Id     [44]  18  "0A0A440200000004"    [1]
    RADIUS:   Cisco AVpair       [1]   36 "parent-session-id=0A0A440200000003"
    RADIUS:  Vendor, Cisco       [26]  21
    RADIUS:   ssg-control-info   [253] 15  "I0;2017511512"
    ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB3 and that is configured with a prepaid service policy.

  Workaround: There is no workaround.

- CSCsh93653

  Symptoms: A router crashes when you configure a local ISG service policy with any routing protocol such as BGP or ISS.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB3 when you enter the following commands:

  ```
  Router(config)#router bgp 1
  Router(config-router)#service
  Router(config-router)#policy-map type service <policy-map-name>
  Router(config-service-policymap)#service local
  ```

  Workaround: Configure and download service profiles via a RADIUS server.

- CSCsh94923

  Symptoms: The PXF engine may crash many times on a Cisco 10000 series that is functions as an L2TP Network Server (LNS). Each time that the PXF engine crashes, the following error message is generated:

  ```
  PXF DMA Error - Input Command Has Sequence Problem.
  ```

  This situation may cause the router to crash (that is, a software-forced crash may occur).

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2 or PRE-3 and that runs Cisco IOS release 12.2(31)SB or one of its rebuilds when packets arrive on an L2TP tunnel and when the inner IP packet is destined for the router. This means that the destination address of the user packet that is carried within the L2TP tunnel is a local address on the LNS. One example of this condition is a keepalive message that is used between the subscriber and the LNS.

  Workaround: The router crashes because IP packets with an L3-destination address are sent to the router over PPP sessions. For packets that arrive on L2TP tunnels, deny access to the IP addresses of the router: on the LNS, configure an input ACL on the virtual template to deny IP access to all router interfaces.

- 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.

- CSCsi03714

  Symptoms: A router may crash when a DLCI configuration is removed from an MFR subinterface.

  Conditions: This symptom is observed on a Cisco 7200 series when the MFR interface has a map class with a service policy attached.

  Workaround: There is no workaround.

- CSCsi10531

  Symptoms: After a PRE switchover has occurred, a PPP interface may not come up. This situation may occur when the PPP interface was shut down and brought up but remained in the up/down state before the PRE switchover occurred.

Conditions: This symptom is observed on a Cisco 10000 series. When the output of the **show ppp interface** command does not show a PPP handle, as in the example below, the symptom has occurred:

```
router#show ppp int p1/0/0
PPP Serial Context Info

Interface         : PO1/0/0
PPP Serial Handle: 0x0
PPP Handle        : 0x0
SSS Handle        : 0x0
AAA ID            : 16
Access IE         : 0x0
State             : Down
Last State        : Init
Last Even           : CstateUp
```

Workaround: After the PRE switchover has occurred, change the interface protocol from PPP to HDLC and then back to PPP to assign a new handle to the interface, as in the following example:

```
conf t
int p1/0/0
encap hdlc
encap ppp
end
```

- CSCsi15221

  Symptoms: A Cisco 7200 series with an NPE-G2 may hang during the boot process.

  Conditions: This symptom is observed when several native Gigabit Ethernet ports with “MV64460” hardware come up simultaneously, for example, while he router boots. To verify if the Gigabit Ethernet ports of your router have “MV64460” hardware, look in the output of the **show interfaces** command.

  Workaround: There is no workaround.

- CSCsi15293

  Symptoms: A new PRE may restart in a continuous loop when you insert it in the standby slot.

  Conditions: This symptom is observed on a Cisco 10000 series when the PRE in the active slot runs a Cisco IOS software image that includes the fix for caveat CSCsf10723.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsf10723. 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.

- CSCsi16819

  Symptoms: An end-to-end ping between CE routers may fail in an ATMoMPLS environment.

  Conditions: This symptom is observed when a Cisco router that functions as a PE router has ATMoMPLS configured as “ATM single cell relay over MPLS: port mode” via the **xconnect** command under an ATM Main interface.

  Workaround: There is no workaround.

- CSCsi19863

  Symptoms: A Cisco 7304 that has an NSE-100 may crash when you unconfigure a match statement in a class map.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(31)SB when you enter the **no match ip prec** twice for a class map.

Workaround: There is no workaround.

- CSCsi20399

  Symptoms: The PXF engine of a Cisco 10000 series may crash and the following error message may be generated:

  ```
  %C10KEVENTMGR-1-MAJOR_FAULT: PXF DMA FTC Move Command with Continue Error PXF DMA
  Error - Input Command Has Sequence Problem, Restarting PXF
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an LNS and that is configured for NetFlow.

  Workaround: Disable NetFlow.

- CSCsi22893

  Symptoms: The statistics that are shown in the output of the **show policy-map session uid** *uid-number* command are not correct for LAC sessions that have QoS enabled.

  Conditions: This symptom is observed on a Cisco 10000 series that runs a Cisco IOS software image that has the fix for caveat CSCsc23981 integrated. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc23981. 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.

- CSCsi25342

  Symptoms: Even after you have removed a T1 line, you still can configure a Facilities Data Link (FDL) on the removed T1 line by entering the **service-module t1 fdl** command. This command should not be accepted since the T1 line is not available.

  Conditions: This symptom is observed on a Cisco 10000 series.

  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.

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

- CSCsi31430

  Symptoms: The Cisco IOS software image on a Cisco 10000 series may unexpectedly reload because of repeated crashes of the PXF engine.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2 and an MLP configuration. The PXF engine may crash each time it reboots, generating more PXF crashinfo files. Eventually, the Cisco IOS software image reloads.

  Workaround: Remove the MLP configuration and/or isolate the router from MLP traffic. If this is not an option, there is no workaround.

- CSCsi32060

  Symptoms: The PXF engine may continuously crash on a Cisco 10000 series.that has a PRE-3.

Conditions: This symptom is observed on a Cisco 10000 series that has an output policer configured on the egress interface when IP packets with a precedence values of 6 are forwarded and when the traffic rate exceeds the value that is configured in the policer.

Workaround: There is no workaround.

- CSCsi46897

  Symptoms: PPP may crash when an **snmpwalk** command is executed on the cbQosSetStatsTable object.

  Conditions: This symptom is observed when a service policy with a child policy that contains marking (“set”) actions is applied to an interface before the **snmpwalk** command is executed on the cbQosSetStatsTable object of the CISCO-CLASS-BASED-QOS-MIB.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCek67998

  Symptoms: Sessions and login authentication may fail on a Cisco 10000 series when a memory allocation (malloc) error occurs that causes the available memory to become low.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for PPPoATM or PPPoEoA when you attempt to change QoS values multiple times with a large number of CoA request for the same session. The symptom does not occur when QoS values are changed a single time or a few times for the same session.

  Workaround: There is no workaround.

- CSCsb83234

  Symptoms: UDP port 1701 (for L2TP) is opened by a port scan. The router does not send a “port unreachable” message for a packet that uses UDP port 1701.

  Conditions: This symptom is observed on a Cisco 1812 router that runs Cisco IOS Release 12.3(14)YT or Release 12.4(2)T1 but may also occur in other releases.

  Workaround: There is no workaround.

- CSCse45182

  Symptoms: When a PPPoE server receives a second PADI from a client (that is, a PADI with the same unique client ID), the PPPoE server may send a PADS with an unknown MAC address.

  Conditions: This symptom is observed on a Cisco platform that functions as a PPPoE server that has established a PPPoE session with a client and occurs while PPP LCP negotiation is in progress.

  Workaround: There is no workaround.

- CSCsi02669

  Symptoms: A router may reload while displaying the output of the **show ppp multilink** command.

  Conditions: This symptom is observed when the multilink bundle goes down while the output is being displayed.

  Workaround: There is no workaround.

- CSCsi08346

  Symptoms: Both accounting START and STOP records are not sent to a RADIUS server after an LNS failover has occurred.

Conditions: This symptom is observed on a Cisco 10000 series that functions as an LNS in a VPDN failover configuration with multihops and that is connected to a RADIUS server. The symptom occurs in a topology in which the LAC has access to both LNS platforms when the first LNS is not accessible but the second LNS is accessible.

Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(31)SB3

Cisco IOS Release 12.2(31)SB3 is a rebuild release for Cisco IOS Release 12.2(31)SB2. This section describes a severity 1 caveat that is open in Cisco IOS Release 12.2(31)SB and its rebuilds. There are other open caveats in Cisco IOS Release 12.2(31)SB3. However, open caveats are normally listed only for maintenance releases, and the listing of CSCsh94923 and CSCsi18240 is an exception.

Miscellaneous

- CSCsh94923

  Symptoms: The PXF engine may crash many times on a Cisco 10000 series that is functions as an L2TP Network Server (LNS). Each time that the PXF engine crashes, the following error message is generated:

  ```
  PXF DMA Error - Input Command Has Sequence Problem.
  ```

  This situation may cause the router to crash (that is, a software-forced crash may occur).

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2 or PRE-3 and that runs Cisco IOS release 12.2(31)SB or one of its rebuilds when packets arrive on an L2TP tunnel and when the inner IP packet is destined for the router. This means that the destination address of the user packet that is carried within the L2TP tunnel is a local address on the LNS. One example of this condition is a keepalive message that is used between the subscriber and the LNS.

  Workaround: The router crashes because IP packets with an L3-destination address are sent to the router over PPP sessions. For packets that arrive on L2TP tunnels, deny access to the IP addresses of the router: on the LNS, configure an input ACL on the virtual template to deny IP access to all router interfaces.

- CSCsi18240

  Symptoms: After receiving packets through an L2TP tunnel and decapsulating these packets, a Cisco 10000 series may corrupt certain packets.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB3. There is a two-byte window for packets that are corrupted:

  - For a PRE-2: if the packet size including all encapsulations prior to L2TP decapsulation is 113 or 114 bytes, respectively, a one- or two-byte corruption of the inner IP packet occurs.
  - For a PRE-3: if the packet size including all encapsulations prior to L2TP decapsulation is 145 or 146 bytes, respectively, a one- or two-byte corruption of the inner IP packet occurs.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs only in Release 12.2(31)SB3 and does not affect other releases.

Resolved Caveats—Cisco IOS Release 12.2(31)SB3

Cisco IOS Release 12.2(31)SB3 is a rebuild release for Cisco IOS Release 12.2(31)SB2. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB3 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCek58840

  Symptoms: When a new PPP session is set up, the following warning message is generated, and the session fails:

  ```
  LAC: %IDMNGR-3-ALLOCFAIL: Warning: Failed to allocate memory for keylist in event_init
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB1. The PPP sessions start failing after the router has been up for about two weeks with many policy-map changes on the PVCs, a few cleared sessions by the clients, and one switchover.

  Workaround: There is no workaround.

- CSCek63810

  Symptoms: A Cisco 10000 series may run out of memory after a number of ATM port flaps have occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with 28,000 PPPoA Point-to-Point Termination and Aggregation (PTA) sessions. Each time that the ATM ports that carry the sessions flap and in this process remain down long enough for the sessions to time-out, more memory is lost.

  Workaround: There is no workaround.

- CSCse42235

  Symptoms: A packet of disconnect (POD) does not disconnect a user. When you enable the **debug aaa pod** command, the output shows the following:

  ```
  POD: Added Reply Message: No Matching Session
  POD: Added NACK Error Cause: Session Context Not Found
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for AAA when the Account-Session-Id is prepended with information. For example, if the Account-Session-Id is “7/0/0/1.40_00000039” in a POD, the POD fails to find a match.

  Workaround: If the Account-Session-Id is “7/0/0/1.40_00000039”, configure the POD application to take only the eight right digits: “00000039”.

- 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.

- CSCsh19482

  Symptoms: A Cisco 10000 series may crash and generate an "%C10K-2-RPRTIMEOUT_CRASH:" error message.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for NetFlow.

  Workaround: There is no workaround.

EXEC and Configuration Parser

- CSCsd45386

  Symptoms: When you enter the **write memory** command, the following error message and a traceback are generated:

  ```
  Router#wr Building configuration...
  % String too long to write to nvram (2578):Compressed configuration from 3452120 bytes
  to 786685 bytes[OK] Uncompressed configuration from 786685 bytes to 3452120 bytes
  ```

  Conditions: This symptom is observed on a Cisco router when the configuration is saved after you have entered the **parser config cache interface** command.

  Workaround: Disable the **no parser config cache interface** command.

Interfaces and Bridging

- 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.

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.

- CSCsc96746

  Symptoms: PIM may not choose the path with the highest IP address when it should do so.

  Conditions: This symptom is observed on a Cisco router that functions in a topology with equal-cost RPF paths.

  Workaround: There is no workaround.

- 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.

- 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.

- 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.

- CSCsh61119

  Symptoms: ARP may be refreshed excessively on the default interface, causing high CPU usage in the "Collection Process."

  Conditions: This symptom is observed on a Cisco router that has point-to-point interfaces that have non-/32 interface addresses or secondary addresses and that constantly come up or go down.

  Workaround: There is no workaround.

ISO CLNS

- CSCsc63871

  Symptoms: When IS-IS and CLNS are configured, a router may enter a state in which only one adjacency is shown in the output of the **show clns interface** command, even though the **show clns neighbors** command may correctly display all the neighbors that are connected to the interface.

  When this situation occurs and any one of the neighbors on the segment goes down, all routing updates may be lost. The single adjacency is torn down and despite the fact that the output of the **show clns neighbors** command still shows the neighbors, routing stops because there are no adjacencies.

  Conditions: This symptom is observed when an adjacency goes down while it is still in the INIT state. The symptom occurs because the adjacency counter is incorrectly decremented.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that reports only one adjacency.

  Alternate Workaround: Enter the **clear clns neighbors** command on the affected router.

Miscellaneous

- CSCdw80441

  Symptoms: A router crashes when you add a new SONET-related interface.

  Conditions: This symptom is observed on a Cisco router when no more memory is available.

  Workaround: There is no workaround.

- CSCej00340

  Symptoms: A Cisco 7304 crashes when you configure an SVC, unconfigure the SVC, configure a VC, and unconfigure the VC.

  Conditions: This symptom is observed on a Cisco 7304 when you perform the following actions:

  1. Configure an SVC, ping another interface, and unconfigure the SVC.
  2. Configure a VC, and ping another interface.
  3. Unconfigure the VC by entering the following commands:

     no ip routing

     no ip address *ip-address mask*

     no atm pvc *vcd vpi vci*

     aal5snap inarp *minutes*

  At this point, the router crashes.

  Workaround: Do not unconfigure a VC by using the method that is indicated in the Conditions above.

  Alternate Workaround: When the router has the **atm bandwidth dynamic** command enabled for an IMA group, remove this command to prevent the router from crashing.

- 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.

- 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.

- CSCek55603

  Symptoms: Spurious memory accesses may occur on a Cisco 10000 series that is configured for PPPoA.

Conditions: This symptom is observed when you first add and then remove Variable Bit Rate (VBR) from a VC class for active PPPoA sessions.

Workaround: There is no workaround.

- CSCek56426

  Symptoms: The police counters are not properly incremented after a class has been added or deleted.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB2 when the total number of classes crosses a power-of-2 boundary after a class has been added to or deleted from the policy that is attached to an interface.

  For example, the symptom occurs under the following conditions:

  - There are 2, 4, 8, or 16 classes in a policy, including the class default, and you add a class.
  - There are 3, 5, 9, or 17 classes in a policy, including the class default, and you delete a class.

  Workaround: Detach the service policy from the interface, add or delete a class to or from the policy, and re-attach the policy.

- CSCek61519

  Symptoms: When you continuously perform OIRs of a SPA or port adapter that is installed in a Port Adapter Carrier Card, tracebacks are generated, and the router eventually crashes.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for HA.

  Workaround: There is no workaround.

- 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.

- CSCek65046

  Symptoms: After a microcode reload has occurred, traffic is dropped for all users that have a per-user ACL configured and for which the user IP address is specified in the ACL.

  Conditions: This symptom is observed on a Cisco 10000 series when a per-user ACL is applied to each session and when an ACL Template is enabled.

  Workaround: After you have performed a microcode reload, disconnect and reconnect all sessions. Note that it is very likely that a user will reconnect a session after traffic has dropped.

- CSCek65838

  Symptoms: The Lawful Intercept feature may not function for active tapped sessions after a microcode reload has occurred. Tapping works fine for new sessions that come up after the microcode reload has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Disconnect and reconnect the existing active tapped sessions after the microcode reload has occurred.

- CSCek67590

  Symptoms: MFR interfaces do not come up when the router boots.

Conditions: This symptom is observed on a Cisco 10000 series that runs a Cisco IOS software image that includes the fix for CSCsg86572 and that has MFR interfaces configured on either a 1 port channelized OC-12 line card or a 4-port channelized OC-3 line card. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg86572. 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.

- CSCir01277

  Symptoms: A Cisco 7304 may reload unexpectedly because of a watchdog reset condition, which can be seen in the output of the **show version** command.

  Conditions: This symptom is observed only on a Cisco 7304 that has an NPE-G100.

  Workaround: There is no workaround.

- CSCsc66658

  Symptoms: A ping does not work when a loopback is configured on an interface.

  Conditions: This symptom is observed on a Cisco 7200 series, Cisco 7500 series, and Cisco 7600 series that are configured with a T3 interface.

  Workaround: There is no workaround.

- CSCsd47447

  Symptoms: A router crashes when a non-VLAN user class is configured under a parent policy with an action such as the **set qos-group** command.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs because a non-VLAN user class under a parent policy is an illegal configuration.

  Workaround: Do not configure a non-VLAN user class under a parent policy. However, note that you can configure a VLAN user class under a parent policy.

- 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.

- 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.

- 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.

- CSCse84099

  Symptoms: When you configure the C2 overhead byte under SONET T3 or VT controllers on a 1-port channelized OC-12/STM-4 or 4-port channelized STM-1/OC-3 line card, the T3 or VT controllers may not come up.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCse98988

  Symptoms: DHCP control messages that are sent by a DHCP relay agent and that are destined for an external DHCP server do not pass through an interface of an Intelligent Service Gateway (ISG).

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when the interface is configured for IP Session Creation.

  Workaround: There is no workaround.

- CSCsf17521

  Symptoms: When a hierarchical policy with CoS is configured, traffic shaping that is applied on the parent policy does not function properly for speeds that are slower than 2000 kbps because the throughput is reduced.

  Conditions: This symptom is observed on a Cisco 7304 when there is a priority class configured in a policy that is attached to an interface. The larger the packets, the more the throughput is reduced.

  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.

- CSCsf20019

  Symptoms: When traffic is being processed at a low speed such as 56 Kbps, intermittently, traffic comes to a complete halt on a Frame Relay subinterface.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2. The symptom occurs when the PXF engine stops dequeueing packets on the Frame Relay subinterface, causing the interface output queue to become wedged.

  Workaround: Remove the service policy from the subinterface and then re-apply the service policy to the subinterface.

  Further Problem Description: Without applying the workaround, about 60 to 70 minutes after the output queue has become wedged, the output queue starts to dequeue itself.

- 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.

- CSCsf97199

  Symptoms: High CPU usage may occur during the "XDR mcast" and "XDR RP" background processes. Each of these processes uses more than 30 percent of the CPU while no data traffic passes through the router.

  Conditions: This symptom is observed on a Cisco 10000 series but is platform-independent.

  Workaround: Reload the router.

- CSCsg15342

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

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

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

- CSCsg44331

  Symptoms: A router may crash when a policy map that is in use by sessions is modified while the sessions are disconnected.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3 but may not be limited to this platform.

  Possible Workaround: Clear all sessions before you modify the policy map.

- CSCsg44431

  Symptoms: A DHCP-initiated IP subscriber session may not respond to DHCP control packets.

Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) when the subscriber session has features enabled that affect the handling of the DHCP control packets.

Workaround: Apply access control lists (ACLs) to the subscriber session to permit bidirectional DHCP control traffic between the ISG and the DHCP client. To do so, enter the **access-list** *access-list-number* **permit udp any any eq bootps** command.

- CSCsg64438

  Symptoms: When a prepaid service is unapplied from rules, the accounting stop record does not contain packet counts and octet counts.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) when the **service-policy type service unapply name** *policy-map-name* command (in which the *policy-map-name* argument indicates the prepaid service) is configured in the rules.

  Workaround for the packet counts: There is no workaround.

  Workaround for the octet counts: Look for the information in the following attributes that are present in the according stop record:

  ```
  ssg-control-info [253] 6 "I<high>;<low>" <low> indicates the input octets.
  ```

  ```
  ssg-control-info [253] 6 "O<high>;<low>" <low> indicates the output octets.
  ```

- CSCsg71200

  Symptoms: During dynamic VLAN class modifications, the queueing policy inheritance fails. This situation causes traffic to be dropped.

  Conditions: This symptom is observed on a Cisco 10000 series that has a hierarchical queueing policy for VLAN classes and a flat shaper for the class default. When the VLAN class modifications occur that shift the matching subinterfaces to the class default, then back to the original VLAN class, and then to another VLAN class, the child queues are not created, causing traffic to drop.

  Workaround: Remove and re-attach the hierarchical queueing policy.

- CSCsg71247

  Symptoms: Non-Priority Queuing (PQ) traffic in a class default in a QoS policy that includes the **match vlan** command is not dequeued during oversubscription of the PQ class.

  Conditions: This symptom is observed on a Cisco 10000 series only when there are multiple VLAN classes and when there are child queueing policies in the class default and the VLAN classes. The PQ policer takes the interface bandwidth as reference, causing policing to occur at the wrong rates and starvation of non-PQ child classes in the class default. The symptom does not occur for child classes in a VLAN class.

  Workaround: There is no workaround.

- CSCsg71400

  Symptoms: Traffic stops matching to a child policy.

  Conditions: This symptom is observed on a Cisco 10000 series when an interface has a hierarchical policy defined on a PVC, when you remove the child policy, and when you re-attach the child policy to the parent policy of the hierarchical policy. In this situation, the traffic no longer matches to the child policy.

  Workaround: Detach the hierarchical policy from the PVC, modify the child policy, and re-attach the hierarchical policy to the PVC.

- CSCsg72950

  Symptoms: Temperature alarms on a Cisco 10000 series PRE-3 assert at lower ambient temperatures than necessary.

  Conditions: This symptom may occur in an operating environment in which the ambient temperature is in the low 30s (degrees Celsius).

  Workaround: You can reprogram the temperature alarm thresholds. The recommended thresholds are:

  ```
  inlet minor: 41 C
  inlet major: 51 C
  inlet critical: 73 C
  outlet minor: 48 C
  outlet major: 58 C
  outlet critical: 85 C
  ```

- CSCsg75132

  Symptoms: When the standby PRE comes up, the following error message is generated on the console of the active PRE:

  ```
  REDUNDANCY-3-IPC: cannot open standby port session in use
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that has dual PRE engines that function in ISSU, RPR+, or SSO mode. The symptom may also occur on other platforms that support Enhanced High System Availability (EHSA) such as the Cisco 7304 and Cisco AS5850.

  Workaround: There is no workaround.

  Further Problem Description: The error message indicates that some of the Entity MIB information such as standby PRE version, standby flash information, and standby EEPROM data has failed to synchronize to the active PRE.

- CSCsg75266

  Symptoms: A Cisco 10000 series with a PRE-3 may crash when you delete an ATM VC.

  Conditions: This symptom is observed when the following sequence of events occur:

  - You enter the **protocol pppoe** command to configure an ATM VC.
  - You enter the **no protocol pppoe** command to remove PPPoE from the VC.
  - You delete the ATM VC.

  Workaround: There is no workaround.

- CSCsg78469

  Symptoms: A Cisco 10000 series may generate an “SW_CORRUPTION” error message when a service of the ISG Layer 4 Redirect feature is removed from a session in a broadband aggregation (BBA) configuration.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an Intelligent Service Gateway (ISG) when a service of the ISG Layer 4 Redirect feature is removed via the configuration of a service policy.

  Workaround: There is no workaround.

- CSCsg89189

  Symptoms: A router may reload when you enter the **show subscriber session detailed** command while sessions are being modified.

Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG).

Workaround: Do not enter the **show subscriber session detailed** command while sessions are being modified.

- CSCsg90929

  Symptoms: When you configure MR-APS between a Cisco 7304 and another router such as a Cisco 7500 series or Cisco 7600 series with PA-MC-STM-1 port adapters, the following tracebacks are logged on the Cisco 7304:

  ```
  -Process= "APS process", ipl= 0, pid= 191
  -Traceback= 406DC2E0 40741174 400C24BC 400C2BF0 400C6D9C 400C79EC 400C8814 400C8894
  400C90B8
  ```

  Conditions: This symptom is observed on a Cisco 7304 when the working or protect PA-MC-STM-1 port adapter in the active state.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs with the following Cisco IOS software images:

  On the Cisco 7304:

  - Release 12.2(28)SB5 (PGP ver.4)
  - Release 12.2(27)SBC5 (PGP ver.4)

  On the Cisco 7600 series:

  - Release 12.2(18)SXD5 (PGP ver.3)
  - Release 12.2(33)SRA1 (PGP ver.4)

- CSCsg95072

  Symptoms: The **show atm vc** command may be missing VCs.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB or a rebuild of Release 12.2(31)SB when at least one ATM line card is installed and VCs are configured.

  Workaround: You can display the ATM VC information by using a more specific command: enter the **show atm vc interface atm** *card/subcard/port* command.

  Further Problem Description: The missing VCs tend to be from select ATM subinterfaces.

- CSCsg97717

  Symptoms: The PXF engine of an NSE-150 crashes when you enter the **ip pim bidir-enable** command.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for MVPN with a single VRF when multicast traffic is flowing through this VRF.

  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.

- CSCsh01626

  Symptoms: A “%SYS-2-MALLOCFAIL” error message may be generated, indicating that there is no free memory available in the router.

  Conditions: This symptom is observed only on a Cisco 7200 series that is configured with an NPE-G2 and that runs a Cisco IOS software image that is based on Release 12.2S.

  Workaround: There is no workaround. To clear the symptom, reboot 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.

- CSCsh04911

  Symptoms: On a Cisco 7304 that is configured for AToM, a software-forced reload may occur on an NSE-100.

  Conditions: This symptom is observed when egress NetFlow is configured on an AToM attachment circuit.

  Workaround: There is no workaround.

  Further Problem Description: The configuration that is stated in the Conditions is essentially a misconfiguration. NetFlow can collect information only about Layer 3 IP packets. However, the AToM attachment circuit is transmitting Layer 2 frames, so the egress NetFlow is not valid.

- CSCsh06611

  Symptoms: A Cisco 10000 series that has a PRE2 may crash when you clean the configuration via TFTP.

  Conditions: This symptom is observed when you first define hierarchical queuing for a QoS VLAN-group policy with a large number of VLAN classes, each class with matching subinterfaces, and then you clean the configuration. The symptom occurs only when you download the configuration via TFTP to the running configuration and when you clean the configuration via TFTP.

  Workaround: There is no workaround.

- CSCsh07031

  Symptoms: L2TP connectivity may not function across the native Gigabit Ethernet interface of an NPE-G2.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(31)SB2 when EIGRP is configured as the routing protocol.

  Workaround: There is no workaround.

- 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.

- CSCsh13739

  Symptoms: The usage of the PXF engine increases to 100 percent. This situation may cause interface flapping, error messages that state that OSPF neighbors are unreachable, and a failure of the standby processor.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with either an NSE-100 or an NSE-150, that has a POS interface that is configured for Frame Relay and that has an output shaping service policy, and that receives traffic that matches the output shaping service policy. In addition, the router is configured with a cross-connect, more specifically, an interface that is configured for Xconnect service and that is connected to a remote peer.

  Workaround: There is no workaround.

- CSCsh13947

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

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

  Workaround: There is no workaround.

- CSCsh15456

  Symptoms: A router may crash when you remove a QoS policy from an interface or modify the policy map.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 when you configure a QoS policy, attach it to the interface, run traffic, and then, after a long time, remove the QoS policy or modify the policy map.

  Workaround: There is no workaround.

- CSCsh24174

  Symptoms: A "%CHKPT-4-INVALID error" error message is generated when you upgrade the Cisco IOS software image to Release 12.2(31)SB.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for ISSU.

  Workaround: There is no workaround.

- CSCsh26001

  Symptoms: When the MIB variable tftpHost is empty (that is, it is not defined), you cannot copy an image via ISSU.

Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB.

Workaround: There is no workaround.

- CSCsh28899

  Symptoms: IS-IS routes are not learned at remote sides.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G2 when the router connects to the remote sides through a native Gigabit Ethernet (GE) interface.

  Workaround: Do not use a native GE interface. Rather, use a GE port adapter such as the PA-GE.

- CSCsh33371

  Symptoms: A static Auto-Rendezvous Point (Auto-RP) may not function when both a Frame Relay main interface and one of its subinterfaces have the **ip pim sparse-dense mode** command enabled.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PE router in an MVPN network.

  Workaround: Remove the **ip pim sparse-dense mode** command from the main interface but leave the **ip pim sparse-dense mode** command enable on the subinterface.

- 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.

- 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.

- CSCsh45466

  Symptoms: A memory leak may occur on a router that is configured with IP ACLs.

  Conditions: This symptom is observed when you enter the **show access-list** command to see a list of ACLs that contains dynamic elements.

  Workaround: There is no workaround.

- CSCsh46427

  Symptoms: A spurious memory access is generated when you remove the **no evaluate tcptraffic** command.

  Conditions: This symptom is observed on a Cisco router that is configured with IP ACLs.

  Workaround: There is no workaround.

- CSCsh46790

  Symptoms: Traffic may no longer be forwarded over a PPPoA session when you remove a policy map from the ATM VC on which the PPPoA session is established.

Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3 when the policy map is applied to the ATM VC and then removed via the **no service-policy output** *policy-map-name* command.

Workaround: There is no workaround.

Further Problem Description: With PPPoA (or PPPoEoA), PXF queues are created on the virtual access interface (VAI) even though the policy map is applied to the VC. When the VC policy map is removed, the default PXF queue is also removed from the VAI, causing a traffic black hole.

- CSCsh47261

  Symptoms: A Cisco 10000 series may either fragment or drop an IPv4 packet when the IPv4 packet length is smaller than the configured MTU. Drops may occur when the DF bit is set in the IPv4 header.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB2 when an ARP cache entry times out or when a static ARP entry is deleted from the configuration.

  Possible Workaround: Increase the MTU of the interface MTU to mitigate the symptom.

  Further Problem Description: The unexpected fragments or packet drops occur in a very short time window after the ARP entry is removed.

- CSCsh51778

  Symptoms: An ISG that receives incorrect VSAs for a policy map may no longer accept any VSAs even if the VSAs are correct.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG and that runs Cisco IOS Release 12.2(28)SB, Release 12.2(31)SB, or Release 12.2(31)SB1.

  Workaround: There is no workaround.

- CSCsh56152

  Symptoms: You cannot suppress the creation of F4 OAM VCs when you configure a PVP at the subinterface level. If the PPP client does not support OAM, this situation could prevent the PPP session from being initiated.

  Conditions: This symptom is observed on a Cisco router and occurs because there is no *no-f4-oam* argument available when you configure a PVP on a subinterface.

  The following command options are available at the main interface level:

  ```
  router(config-if)#atm pvp 2 10000 ?
  cdvt           [Cell Delay Variation Tolerance (CDVT)]
  no-f4-mgmt     [inhibits the management of f4 oam vcs]
  no-f4-oam      [inhibits the creation of f4 oam vc's]
  cr
  ```

  However, only the following options are available at the sub interface level:

  ```
  router(config-if)#atm pvp 2 10000 ?
  cdvt           [Cell Delay Variation Tolerance (CDVT)]
  cr
  ```

  Workaround: Do not configure the PVP on the subinterface. Rather, configure the PVP on the main interface, for which the *no-f4-oam* argument is available.

- CSCsh63369

  Symptoms: All traffic that arrives on a PPP over VLAN session or PPPoE over QinQ session may be processed indiscriminately by the class default of a service policy that is applied to the VLAN or QinQ VLAN.

  Conditions: This symptom is observed on a Cisco 10000 series that runs a Cisco IOS software image that integrates the fix for caveat CSCsg89172. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg89172. 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.

TCP/IP Host-Mode Services

- CSCsc39357

  Symptoms: A Cisco router may drop a TCP connection to a remote router.

  Conditions: This symptom is observed when an active TCP connection is established and when data is sent by the Cisco router to the remote router at a much faster rate than what the remote router can handle, causing the remote router to advertise a zero window. Subsequently, when the remote router reads the data, the window is re-opened and the new window is advertised. When this situation occurs, and when the Cisco router has saved data to TCP in order to be send to the remote router, the Cisco router may drop the TCP connection.

  Workaround: Increase the window size on both ends to alleviate the symptom to a certain extent. On the Cisco router, enter the **ip tcp window-size** *bytes* command. When you use a Telnet connection, reduce the *screen-length* argument in the **terminal length** *screen-length* command to 20 or 30 lines.

- 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.

Wide-Area Networking

- CSCsf29303

  Symptoms: On a Cisco 7200 series, an error message and traceback such as the following are generated and/or the router may crash because of an "%ALIGN-1-FATAL: Illegal access to a low address" condition:

  ```
  %SYS-2-BADSHARE: Bad refcount in retparticle, ptr=652AA0C0, count=0
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x621FD418 reading 0x278
  ```

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(31)SB when end-to-end Frame Relay fragmentation is configured on an interface.

Workaround: Do not configure end-to-end Frame Relay fragmentation. Rather, configure end-to-end fragmentation that is based on a map class, that is, attach to each PVC a map class that contains an end-to-end fragmentation configuration.

- CSCsg56725

  Symptoms: When you enter the **terminate-from hostname** *host-name* command to terminate L2TP tunnels, some L2TP tunnels are terminated in the wrong VPDN group while other L2TP tunnels on the same host are terminated in the correct VPDN group.

  Conditions: This symptom is observed on a Cisco 7206VXR that has an NPE-G1 and that runs Cisco IOS Release 12.2SB and occurs only during the first two or three minutes after the router has booted. After that period, the symptom no longer occurs. Note that the symptom is both platform- and release-independent.

  Workaround: To prevent the symptom from occurring, enter the **no aaa accounting system guarantee-first** command on the router before you reload the router. Doing so enables the tunnels to be terminated in the correct VPDN groups.

  After the symptom has occurred, clear each of the affected tunnels by entering the **clear vpdn tunnel id** *local-id* command. Then, after the tunnels have been re-established, you should be able to terminate them in the correct VPDN groups.

- CSCsh49699

  Symptoms: A router may crash when you configure Frame Relay fragmentation on a Frame Relay main interface after the following error message has been generated:

  ```
  "Leased-line fragmentation works with main interface service-policy only, please
  remove policy under subinterface/PVC and re-enter the command."
  ```

  Conditions: This symptom is observed on a Cisco router after you first have attempted to configure Frame Relay fragmentation on a Frame Relay main interface that has a service policy on a subinterface, when you then have removed the service policy from the subinterface, and when you then again attempt to configure Frame Relay fragmentation.

  Workaround: After the error message has been generated, immediately remove the Frame Relay fragmentation before you remove the service policy.

- CSCsh62833

  Symptoms: The **sessions per-mac throttle** command functions as expected, but when you enter the **show pppoe throttled mac** command, no output is displayed, and a warning message and traceback are generated:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0  data 70A48450
  chunkmagic 0  chunk_freema0
  -Process= "Exec", ipl= 0, pid= 234
  -Traceback= 6053AADC 606167A8 6158DB78 61578A28 61578B4C 604E4BF4 601C01E8
  604FE6F8 60617B54 60617B40
  604FE6F8 60617B54 60617B40
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that has an PRE-2, that runs Cisco IOS Release 12.2(28)SB4, and that is configured for PPPoE Connection Throttling. Note, however, that the symptom is not platform-specific.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(31)SB2

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(31)SB2. All the caveats listed in this section are open in Cisco IOS Release 12.2(31)SB2. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCse42235

  Symptoms: A packet of disconnect (POD) does not disconnect a user. When you enable the **debug aaa pod** command, the output shows the following:

  ```
  POD: Added Reply Message: No Matching Session
  POD: Added NACK Error Cause: Session Context Not Found
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for AAA when the Account-Session-Id is prepended with information. For example, if the Account-Session-Id is "7/0/0/1.40_00000039" in a POD, the POD fails to find a match.

  Workaround: If the Account-Session-Id is "7/0/0/1.40_00000039", configure the POD application to take only the eight right digits: "00000039".

- CSCsg74449

  Symptoms: When a PVC with a policy map is unconfigured on a 1-port OC-12 ATM line card, a Cisco 7304 with an NSE-100 crashes and generates an "ALIGN-1-FATAL" error message.

  Conditions: This symptom is observed on a Cisco 7304 that functions as both a core router and a route reflector (RR) when you unconfigure the PVC while traffic is being processed.

  Workaround: There is no workaround.

EXEC and Configuration Parser

- CSCsd45386

  Symptoms: When you enter the **write memory** command, the following error message and a traceback are generated:

  ```
  Router#wr Building configuration...
  % String too long to write to nvram (2578):Compressed configuration from 3452120 bytes
  to 786685 bytes[OK] Uncompressed configuration from 786685 bytes to 3452120 bytes
  ```

  Conditions: This symptom is observed on a Cisco router when the configuration is saved after you have entered the **parser config cache interface** command.

  Workaround: Disable the **no parser config cache interface** command.

IP Routing Protocols

- CSCek39951

  Symptoms: CPUHOG messages are generated when the standby RP boots with a very large configuration such as more than 1000 BGP peers.

  Conditions: This symptom is observed on a Cisco 10000 series with a PRE-3 when the *milliseconds* argument of the **process-max-time** *milliseconds* command has a value of 50 ms. The symptom is platform-independent.

Workaround: There is no workaround.

- CSCek57267

  Symptoms: CPUHOG and IPCOIR errors may occur on a Cisco router when you change the IP address of a loopback interface that is associated with a large number of active PPP sessions.

  Conditions: This symptom is observed on a Cisco 10000 series that runs slowly when interfaces flap. The symptom is platform-independent.

  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.

- CSCsc32700

  Symptoms: A router may not resume to forward VPN traffic after you have entered the **redundancy force-switchover** command.

  Conditions: This symptom is observed on a Cisco router that function as a PE router in a VPN environment.

  Workaround: There is no workaround.

- CSCsc37461

  Symptoms: A PE router that functions in an MPLS VPN configuration may take a long time to converge.

  Conditions: This symptom is observed when an interface goes down and when an MP-BGP next hop that points to this interface is no longer reachable. This MP-BGP next hop remains unreachable until the Interior Gateway Protocol (IGP) finds an alternate path. If the BGP scanner runs while the MP-BGP next hop is unreachable, VRF routes that use this MP-BGP next hop may be removed from the VRF routing table. However, usually, when the next BGP scanner runs, these VRF routes are updated and then re-imported into VRF routing table.

  Workaround: The probability for the symptom to occur depends on the elapse time between the interface going down and the IGP convergence and can be decreases by tuning the IGP parameters for a faster convergence.

- CSCsd39528

  Symptoms: Duplicate Interface Index (ifIndex) numbers may be assigned to the multicast tunnel interfaces. This situation may prevent traffic from being switched from these multicast interfaces, and may cause the router to crash with a bus error when these multicast tunnels are deleted and then re-created.

  You can verify that the symptom has occurred by entering the **show idb** command and by looking for duplicate ifIndex entries for the multicast tunnel interfaces.

  Conditions: This symptom is observed on a Cisco router that is configured with IPv6 PIM tunnels.

  Workaround: There is no workaround.

- CSCsg07742

  Symptoms: The attributes that are configured in a site map may not automatically be applied to the BGP table when the associated interface is running other routing protocols such as RIP or OSPF.

  Conditions: This symptom is observed on a Cisco router when routes are redistributed into BGP.

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

- CSCsg25995

  Symptoms: Networks do not show in the Multiprotocol BGP (MBGP) table, as can be seen in the output of the **show ip mbgp** command.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB, Release 12.4, or Release 12.4T.

  Workaround: Enter the **clear ip bgp** *neighbor-address* command to enable the networks to enter the MBGP table.

- CSCsg78768

  Symptoms: Multiprotocol BGP (mBGP) peers may not receive modified cost-community routes.

  Conditions: This symptom is observed on a Cisco router after route maps have been applied. The router checks if the modified routes are sent to its peers. However, the multicast peers do not receive the modified routes.

  Workaround: There is no workaround.

  Further Problem Description: The routes are sent properly to unicast and VPN peers.

- CSCsg84949

  Symptoms: After a router has booted, BGP links start to flap, and the router crashes.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router, that is connected to a route reflector (RR), and that is configured with 500 VRFs and 500 routes per VRF.

  Workaround: There is no workaround.

Miscellaneous

- CSCdy19642

  Symptoms: Performance counters under T1.5, T3, and VT2 controllers for T1 and E1 interfaces on a channelized line card are not properly updated and displayed.

  Conditions: This symptom is observed on a Cisco 10000 series when cyclic redundancy check (CRC) errors occur.

  Workaround: There is no workaround.

- CSCeh04362

  Symptoms: Routed Bridge Encapsulation (RBE) does not function in an IPv6 environment.

  Conditions: This symptom is observed on a Cisco router when traffic attempts to pass through an interface that is configured for both RBE and IPv6.

  Workaround: There is no workaround.

- CSCeh71337

  Symptoms: Traffic loss may occur for more than 80 seconds after a high availability (HA) switchover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that has line cards that are configured for Automatic Protection Switching (APS).

  Workaround: There is no workaround.

- CSCeh92464

  Symptoms: The output of the **show policy-map** command may show incorrect WRED counters.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that has DSCP-based WRED enabled.

  Workaround: There is no workaround.

- CSCej02774

  Symptoms: When you use the **BREAK** key to interrupt the image boot process and then enter the **dir** command from the ROMmon prompt, a recurring "Arithmetic Overflow Exception" may occur.

  Conditions: This symptom is observed on a Cisco 10000 series that has 104480 Kbytes of main memory and occurs only when a file system device driver is recursively loaded because you used the **BREAK** key to interrupt the image boot process and then entered the **dir** command without first resetting the ROMmon.

  Workaround: Let the image boot and then enter the **dir** command. If you must interact with the file system via the ROMmon when the boot process has been interrupted, enter the **reset** command. If autoboot is enabled, use the **BREAK** key immediately after the banner line appears on screen.

- CSCej07319

  Symptoms: A router may crash when you configure Mobile IP.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.12SB or Release 12.2SBC.

  Workaround: There is no workaround.

- CSCej62041

  Symptoms: The following symptoms may occur:

  - When a service policy for traffic shaping is applied to an mGRE tunnel interface, most of the packets are dropped.
  - When a service policy is applied to an outbound physical interface, very few or none of the packets are matched, policed, and/or shaped, or the queuing features do not function.

  Conditions: This symptom is observed when multicast fast switching is configured over mGRE tunnels.

  Workaround: There is no workaround.

- CSCej66992

  Symptoms: The statistic counters for a parent policy and for parts of a child policy may be incorrect in the output of the **show policy-map interface** *interface-name* command.

  Conditions: This symptom is observed on a Cisco 10000 series when an egress policy map is attached to an interface, when the egress policy map has a nested child service policy, and when you modify class maps in the child policy.

  Workaround: Remove the child policy map from the parent policy map before you modify the child class maps. Then, re-attach the child policy to the parent.

- CSCek19916

  Symptoms: When more than 100 pseudowire (PW) VCs are brought down simultaneously, enqueue failures occur, preventing PWE3-MIB notifications from being sent for the PW VCs beyond the first 100 PW VCs that went down.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs because the notification queue of the PWE3-MIB is full.

Workaround: Configure a network management station (NMS) to report that a state change occurs for PW VCs, for example, via the MPLS-LDP-MIB.

- CSCek20073

  Symptoms: A Cisco 10000 series may reload unexpectedly during HA configuration synchronization operations.

  Conditions: This symptom is observed very rarely on a Cisco 10000 series that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCek24445

  Symptoms: A Cisco 10000 series that has a scaled configuration may crash when an SSO switchover occurs.

  Conditions: This symptom is observed on a Cisco 10000 series that functions in the following large Remote Access (RA) to MPLS VPN configuration:

  - 250 PPPoA sessions over one VPN.
  - 500 MPLS VPNs with eBGP
  - 500 L2vPNs (EoMPLS) VCs
  - 200 ATMoMPLS sessions
  - 200 FRoMPLS sessions
  - mVPN on T1, E1, and MLP links
  - MPLS TE tunnels
  - IPv4 and IPv6 tunnels

  Workaround: There is no workaround.

- CSCek35534

  Symptoms: Packet loss may occur on voice or video streams when you apply an output policy on the interface.

  Conditions: This symptom is observed on a Cisco 10000 series when traffic is sent at line rate.

  Workaround: There is no workaround.

- CSCek36747

  Symptoms: When Internet mix (IMIX) traffic is processed over an L2VPN pseudowire that is configured for shaping on a disposition PE router, shaping does not function as expected, causing packets to be dropped.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a disposition PE router.

  Workaround: There is no workaround.

- CSCek41565

  Symptoms: The maximum latency of priority queueing (PQ) may be too high for some ports.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCek41755

  Symptoms: The on-demand address pool (ODAP) manager does not create the required number of subnets.

  Conditions: This symptom is observed on a Cisco router that has the DHCP ODAP Server Support feature enabled.

  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.

- CSCek43707

  Symptoms: When an interface is configured for Routed Bridge Encapsulation (RBE) and Dynamic Host Control Protocol (DHCP) and when an HA switchover occurs, routes do not synchronize on the new standby RP.

  Conditions: This symptom is observed on a Cisco 10000 series after you have performed an OIR of the interface that is configured for RBE and DHCP. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCek44091

  Symptoms: An MPLS tunnel goes down after you have changed the tunnel priority from 3 to 2 via the **tunnel mpls traffic-eng priority** command.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- 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.

- CSCek49107

  Symptoms: A router crashes when you unconfigure and then reconfigure MLPoFR.

  Conditions: This symptom is observed on a Cisco router that has a QoS service policy with traffic shaping.

  Workaround: There is no workaround.

- CSCek49973

  Symptoms: When Multilink PPP (MLP) is configured to use a virtual access interface as the bundle interface and when you apply a service policy with bandwidth guarantees that are higher than the bandwidth guarantees of the virtual access interface, an error message is generated because the service policy is not rejected nor enters the suspended mode.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB and that is configured for MLP and QoS.

  Workaround: Add more links to the bundle interface and clear the virtual access interface.

- CSCek52663

  Symptoms: Memory failures may occur on a Cisco 10000 series when you repeatedly perform OIRs.

  Conditions: This symptom is observed very rarely on a Cisco 10000 series that runs Cisco IOS Release 12.2SB after repeated OIRs of a line card that is configured for Auto VCs and that has active PPPoA sessions.

  Workaround: There is no workaround.

- CSCek52743

  Symptoms: cRTP may become disabled on an interface when you disable and re-enable the **ip rtp header-compression** command on the interface.

  Conditions: This symptom is observed on a Cisco router that functions in an MLP configuration when the link (such as a Frame Relay link) and the MLP bundle clone from the same virtual template.

  Workaround: Reset the interface.

- CSCek53834

  Symptoms: When you repeatedly clear PPPoA sessions, memory may become fragmented, and eventually may become so low and fragmented that you cannot execute the **show running-config** command.

  Conditions: This symptom is observed on a Cisco 10000 series when you repeatedly clear PPPoA PTA sessions by entering the **clear pppatm** command.

  Workaround: There is no workaround.

- CSCek55603

  Symptoms: Spurious memory accesses may occur on a Cisco 10000 series that is configured for PPPoA.

  Conditions: This symptom is observed when you first add and then remove Variable Bit Rate (VBR) from a VC class for active PPPoA sessions.

  Workaround: There is no workaround.

- CSCek56426

  Symptoms: The police counters are not properly incremented after a class has been added or deleted.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB2 when the total number of classes crosses a power-of-2 boundary after a class has been added to or deleted from the policy that is attached to an interface.

  For example, the symptom occurs under the following conditions:

  - There are 2, 4, 8, or 16 classes in a policy, including the class default, and you add a class.
  - There are 3, 5, 9, or 17 classes in a policy, including the class default, and you delete a class.

Workaround: Detach the service policy from the interface, add or delete a class to or from the policy, and re-attach the policy.

- CSCek59453

  Symptoms: When you configure an ATM VC on which PPPoE sessions are established, a spurious memory access may be generated.

  Conditions: This symptom is observed on a Cisco router when the VC is torn down.

  Workaround: There is no workaround.

- CSCsc74782

  Symptoms: The number of BECN-tagged packets that are sent by one CE router does not match the number of BECN-tagged packets that are received by another CE router. This symptom can be verified in the output of the **show frame-relay pvc** command.

  Conditions: This symptom is observed under the following conditions:

  - Both CE routers are connected to PE routers.
  - One of the PE routers is a Cisco 10000 series and the other PE router is a Cisco 7500 series.
  - There is an AToM tunnel between the PE routers and the AToM tunnel was set via Xconnect commands.
  - The AToM tunnel is configured for DLCI-to-DLCI switching.

  Workaround: There is no workaround.

- CSCsd23425

  Symptoms: QoS statistics are not reflected properly in the output of the **show policy-map session uid** *uid-number* command.

  Conditions: This Symptom is observed on a Cisco 10000 series is has a PRE2 and that functions as a LAC.

  Workaround: There is no workaround.

- CSCsd47447

  Symptoms: A router crashes when a non-VLAN user class is configured under a parent policy with an action such as the **set qos-group** command.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs because a non-VLAN user class under a parent policy is an illegal configuration.

  Workaround: Do not configure a non-VLAN user class under a parent policy. However, note that you can configure a VLAN user class under a parent policy.

- CSCsd82031

  Symptoms: I/O memory may become depleted on a Cisco 7304 because of IPC buffer usage. This situation may also cause the following error messages to be generated:

  ```
  %WSIPC-3-SYSCALL: System call for command 7 (port 4/1): ipc_send_rpc_blocked
  timed-out (Cause: timeout)
  -Traceback= 406EB43C 40924448 409245FC 40924750
  ```

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and three Port Adapter Carrier Cards (7300-CC-PAs) in which 8-port serial, X.21 port adapters (PA-8T-X21) are installed and occurs when many serial interfaces are reset.

  Workaround: Prevent the serial interfaces from being reset.

- CSCse14947

  Symptoms: A standby RP may continuously reload after you have entered the **redundancy force-switchover** command.

  Conditions: This symptom is observed on a Cisco router that has the **atm pvp** *vpi* **l2transport** interface configuration command enabled for an AToM tunnel that functions in ATM PVP mode.

  Workaround: Disable the **atm pvp** *vpi* **l2transport** interface configuration command. When you do so, the standby RP comes back up.

- CSCse21604

  Symptoms: When a failure occurs on a CE router, the primary pseudowire switches over to the backup pseudowire. However, when the failure is corrected, the backup pseudowire does not fall back to the primary pseudowire but remains in the “UP” state.

  Conditions: This symptom is observed on a Cisco router that functions as a CE router when the ATM-to-ATM Local Switching and L2VPN Pseudowire Redundancy features are configured with an AToM (like-to-like) pseudowire class. The symptom occurs only in an ATM configuration.

  Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface that faces the PE router. Doing so forces the primary pseudowire to come up.

- CSCse29304

  Symptoms: The call setup rate on an LNS may be very slow.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an LNS.

  Workaround: There is no workaround.

- CSCse30504

  Symptoms: A CPUHOG condition may cause an interface of an OC-12 port line card to flap even though the remote link is still active.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCse41607

  Symptoms: All ingress traffic into a Gigabit Ethernet (GE) SPA may be ignored.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 or NSE-150 when the following conditions are present:

  - PXF is disabled.
  - The router has an MSC-100 in which a GE SPA is installed.
  - The router processes traffic at GE rate (or, at a rate that causes the CPU usage of the NSE to be at 100 percent).
  - You perform a series (at least 5 or 6) of physical OIRs of the MSC-100.

  You must reload the router to recover proper functionality.

  Workaround: Enable PXF.

  Alternate Workaround: Do not perform a series of consecutive physical OIRs of the MSC-100 while traffic is being switched and the CPU usage of the NSE is at 99 or 100 percent.

- CSCse55371

  Symptoms: A policing error may occur on a DHCP IP session when local authorization is configured.

Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG).

Workaround: Configure a static IP session and RADIUS authorization.

- CSCse59604

  Symptoms: The CPU of a router may spike when an empty control policy is configured on an interface and when another non-empty control policy is configured at either the global or the interface level.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG).

  Workaround: Do not configure an empty control policy on the interface.

- CSCse78015

  Symptoms: When you change the MTU on a virtual template, an incorrect value is used for the IP MTU.

  Conditions: This symptom is observed when the value that is set as the MTU via the **mtu** *bytes* command is automatically entered as the maximum value for *bytes* argument of the **ip mtu** *bytes* command.

  This symptom occurs only with MTU values in the range of 64 to 67 when an IP MTU is also configured. MTU values from 68 up to the interface maximum work fine. Some interfaces allow a minimum MTU value of 64 but the minimum IP MTU value is 68, therefore, MTU values in the range of 64 to 67 may cause a problem.

  For example, when you change the MTU via the **mtu** *bytes* command to a minimum value of 64 while the IP MTU has a minimum value of 68, the IP MTU is automatically changed to a maximum value of 64, which causes the IP MTU to cover an incorrect range.

  Workaround: Avoid MTU values in the range from 64 to 67.

- CSCse83462

  Symptoms: CEF convergence takes a long time in a load-balancing configuration on a Cisco 10000 series that has a PRE-3.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PE router in an MPLS VPN configuration and that is connected to two P routers. The symptom occurs after an interface has flapped.

  Workaround: There is no workaround.

- CSCse84099

  Symptoms: When you configure the C2 overhead byte under SONET T3 or VT controllers on a 1-port channelized OC-12/STM-4 or 4-port channelized STM-1/OC-3 line card, the T3 or VT controllers may not come up.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCse98988

  Symptoms: DHCP control messages that are sent by a DHCP relay agent and that are destined for an external DHCP server do not pass through an interface of an Intelligent Service Gateway (ISG).

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when the interface is configured for IP Session Creation.

  Workaround: There is no workaround.

- CSCsf02261

  Symptoms: Multilink PPP (MLP) traffic fails when it is forwarded via a LAC (or LNS) over an PPPoA session.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a LAC and that runs Cisco IOS Release 12.2(28)SB2. The symptom occurs when the MLP traffic comes from an ADSL router via an L2TP session and when the CPE connects to the LAC via PPPoA.

  Workaround: Configure the CPE to connect to the LAC via PPPoEoA instead of PPPoA.

- CSCsf20019

  Symptoms: When traffic is being processed at a low speed such as 56 Kbps, intermittently, traffic comes to a complete halt on a Frame Relay subinterface.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2. The symptom occurs when the PXF engine stops dequeueing packets on the Frame Relay subinterface, causing the interface output queue to become wedged.

  Workaround: Remove the service policy from the subinterface and then re-apply the service policy to the subinterface.

  Further Problem Description: Without applying the workaround, about 60 to 70 minutes after the output queue has become wedged, the output queue starts to dequeue itself.

- CSCsf20691

  Symptoms: When an unknown Change of Authorization (CoA) service policy is pushed to an active ISG session, the service policy is not acknowledged and the ISG session is terminated.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG. The following is an example of the conditions under which the symptom occurs:

  A CoA service policy is pushed in the following VSA format:

  ```
  vsa cisco generic 1 string "subscriber:policy-directive=service-policy type service
  name BOOTONE"
  ```

  The BOOTONE service does not exist in the local ISG profile database, nor in the AAA service database.

  Workaround: There is no workaround.

- CSCsf28509

  Symptoms: When you enter the **clear ip dhcp binding** command to clear DHCP bindings, the corresponding DHCP-initiated subscriber sessions are not cleared.

  Conditions: This symptoms is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG).

  Workaround: Enter the **clear ip subscriber** command to clear the subscriber sessions.

- CSCsg09230

  Symptoms: When traffic is processed over a session after you have removed the standby RP, a memory leak may occur in the an “adj_allocate_setup_and_lock” process.

  Conditions: This symptom is observed on a Cisco router that is configured for PTA and L2TP sessions.

  Workaround: Do not remove the standby RP after you have booted the router.

- CSCsg10730

  Symptoms: A multicast ping packet that is sent from one CE router to another CE router may be dropped.

Conditions: This symptom is observed on a Cisco 7304 and Cisco 10000 series that function in a Multicast VPN (MVPN) configuration with Autonomous System Border Routers (ASBRs).

Workaround: There is no workaround.

Further Problem Description: The symptom does not occur on a Cisco 7200 series.

- CSCsg18588

  Symptoms: A router may be unable to bring up more than 36,000 sessions in a configuration with VC-classes and QoS policy maps. Memory errors may be reported and sessions may be disconnected.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG and occurs only when all of the following criteria are present:

  - There are more than 38,000 VCs configured.
  - The VCs have VC-classes.
  - The VCs have outbound policy maps configured.

  Workaround: There is no workaround.

- CSCsg22762

  Symptoms: The cache entries of Flexible NetFlow may lock up for multicast traffic.

  Conditions: This symptom is observed during normal Flexible NetFlow operation when multicast traffic enters the router.

  Workaround: There is no workaround.

- CSCsg23257

  Symptoms: Duplication or tapping does not occur on a Cisco 7301 that is configured for Lawful Intercept (LI).

  Conditions: This symptom is observed when a PPPoE session is set up at the client and when you attempt to duplicate packets at a Cisco 7301 that functions as a LAC and that is configured for LI. The symptom is platform-independent.

  Workaround: There is no workaround.

- CSCsg25018

  Symptoms: The working interface is not restored to the active state but remains inactive while the protect interface remains active in the following situation:

  - The working interface has the **pos ais-shut command enabled.**
  - You enter the **aps revert** command to enable a switchover from the protect interface to the working interface.
  - You enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the working interface.

  The working interface should become active but does not do so.

  Conditions: This symptom is observed on a Cisco 7304 when interfaces of an OC-3 POS line card are configured for APS and occurs only in a back-to-back bi-directional APS configuration. The symptom does not occur with an OC-3 POS port adapter.

  Workaround: Perform a soft OIR of the working interface.

  Alternate Workaround: Disable the **pos ais-shut command on the working interface.**

  Possible Workaround: Enter the **pos scramble-atm** on the active interface. Note that this workaround does not always work.

- CSCsg32170

  Symptoms: When dynamic bandwidth selection (DBS) is enabled on an ATM VC, policing on PPPoX sessions may exceed the configured policing rates.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an Intelligent Service Gateway (ISG) when the following sequence of events occurs:

  1. Configure a QoS policy in the egress direction on the ATM VC that has DBS enabled.
  2. Bring up a PPPoX session and download the QU and QD values of the account information at the start of the session.
  3. Bring up one more new session and then tear down this session.

  After you have torn down the second session, traffic flowing through the first session may exceed the policing values that have been configured.

  Workaround: Disable DBS on the interface on which the ATM VC is configured.

- CSCsg32465

  Symptoms: Incorrect police percent conversions occur in the second and third levels of a policy.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2SB. However, the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCsg34025

  Symptoms: A Cisco 7206VXR crashes because of a software bus error when the main interface is shut down and brought up again.

  Conditions: This symptom is observed on a Cisco 7206VXR with an NPE-G1 that runs Cisco IOS Release 12.2(28)SB5 and that has a Frame Relay map class with a QoS service policy that is applied to an MFR subinterface.

  Workaround: Remove the Frame Relay map class from the MFR subinterface.

- CSCsg38900

  Symptoms: The PXF engine on an NSE-150 may crash at PXF column 2 when a switchover occurs while traffic is being processed. When this situation occurs, no information is written to the crashinfo file.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for HA, that has 250 FEC VRFs, and that has the **ip cef** and **ip pxf** commands enabled.

  Workaround: Do not enable the **ip cef** command in an HA configuration. Rather, enable the **ip cef distributed** command.

- CSCsg38944

  Symptoms: The following error message is generated when a PVC is shut down.

  ```
  %ATM-3-FAILMODIFY VC: failed to modify messages in the log
  ```

  Conditions: This symptom is observed on a Cisco 10008 when a PVC is shut on the remote side.

  Workaround: There is no workaround.

- CSCsg44331

  Symptoms: A router may crash when a policy map that is in use by sessions is modified while the sessions are disconnected.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3 but may not be limited to this platform.

Possible Workaround: Clear all sessions before you modify the policy map.

- CSCsg44431

  Symptoms: A DHCP-initiated IP subscriber session may not respond to DHCP control packets.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) when the subscriber session has features enabled that affect the handling of the DHCP control packets.

  Workaround: Apply access control lists (ACLs) to the subscriber session to permit bidirectional DHCP control traffic between the ISG and the DHCP client. To do so, enter the **access-list** *access-list-number* **permit udp any any eq bootps** command.

- CSCsg50129

  Symptoms: The PA-CC on a Cisco 7304 that has an NSE-100 may crash when you enter the **clear interface atm** command more than once for the interface of a 1-port ATM OC-3c/STM-1 multimode, enhanced port adapter (PA-A6-OC3MM) that is installed in the PA-CC.

  Conditions: This symptom is observed on a Cisco 7304 when the PA-A6-OC3MM is configured with 500 VRFs, when traffic is passing through all the VRFs, and when not all VCs have come up after the previous **clear interface atm** command was entered while you enter the **clear interface atm** command again.

  Workaround: After you have entered the **clear interface atm** command, wait for all the VCs to come up before you enter the **clear interface atm** command again.

  Alternate Workaround: Do not enter the **clear interface atm** command. Rather, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface of the PA-A6-OC3MM.

- CSCsg50211

  Symptoms: A Gigabit Ethernet connection between a Gigabit Ethernet port on a Cisco 10000 series and another platform may become inoperative unexpectedly.

  Conditions: This symptom is observed randomly on a Cisco 10000 series that runs Cisco IOS Release 12.2SB and that has an interface that is configured for auto-negotiation on a full-height or half-height Gigabit Ethernet line card.

  Possible Workarounds: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface. If this workaround does not clear the symptoms, enter the **hw-module reset** command for the affected line card. If neither of these workarounds clear the symptoms, reload the router.

- CSCsg53878

  Symptoms: An invalid traceback address may be displayed as part of a CPUHOG error message, as in the following example:

  ```
  %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (6/6),process
  = Virtual Exec. -Traceback= BFC30E70
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3 and that runs Cisco IOS Release 12.2(31)SB2 when commands are entered from the virtual terminal.

  Workaround: There is no workaround.

  Further Problem Description: When the symptom occurs, collect the output of the **show processes cpu sorted | ex 0.00** command. Then, for the processes that have a high CPU usage as shown in the output of the **show processes cpu sorted | ex 0.00** command, enter the **show stack** *#* command and substitute the PID of the output of the **show processes cpu sorted | ex 0.00** command for the *#* argument in the **show stack** *#* command. Then, submit all output to the Cisco Technical Assistance Center (TAC) for further assistance.

- CSCsg53975

  Symptoms: An OC-3 POS interface on a Cisco 10000 series that is connected to a Cisco 7200 series remains in the down/down state after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the OC-3 POS interface.

  Conditions: This symptom is observed on a Cisco 10000 series that has a 6-port OC-3 POS line card.

  Workaround: Reload the Cisco 10000 series.

- CSCsg58029

  Symptoms: CPU usage may be at 100 percent for more than 10 minutes, and all line cards may reboot.

  Conditions: These symptoms are observed very rarely on a Cisco 10000 series when a large number of links on the router flap while traffic is being processed.

  Workaround: There is workaround.

- CSCsg58896

  Symptoms: A Cisco 10000 series that is configured for PPP may crash because of memory corruption.

  Conditions: This symptom is observed rarely on a Cisco 10000 series when a large number of serial links flaps during a long period of time, causing multilink bundles to go up and down.

  Workaround: There is no workaround.

- CSCsg66504

  Symptoms: Traffic is lost for 10 to 15 seconds after a PRE switchover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series immediately after the standby PRE enters the hot standby state.

  Workaround: There is no workaround.

- CSCsg68753

  Symptoms: When you configure a traffic class to classify traffic on precedence 2 with a mark probability denominator of 1/5 and on precedence 6 with a mark probability denominator of 1/10, the output of the **show policy-map interface** command shows that the mark probability denominator for both precedence values is 1/10.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(28)SB2 and that is configured for WRED.

  Workaround: There is no workaround.

- CSCsg69691

  Symptoms: When a microcode reload is performed, the router may crash and generate the following error message:

  ```
  %ERR-1-GT64120 (PCI-1): Fatal error, PCI Master abort
  ```

  Conditions: This symptom is observed on a Cisco 10000 series when you enter the **microcode reload all** command.

  Workaround: There is no workaround.

- CSCsg70687

  Symptoms: A Port Adapter Carrier Card (CC-PA) on a Cisco 7304 may crash and generate the following error messages and tracebacks in the logs:

  ```
  %WSIPC-3-SYSCALL: System call for command 7 (port 2/0) : ipc_s end_rpc_blocked
  timed-out (Cause: timeout)
  -Traceback= 406F016C 40929BC4 40929D78 40929ECC

  %LC-3-RECOVERY: Line card (slot 2) recovery in progress
  -Traceback= 406F016C 408B9028 401F3680 408C017C 4087FAE4 408645E4 407F1E64

  %LC-3-SANTAANA: Santa Ana Asic: NSE instance 0, Serial Channel A (slot 2), Error
  Status 0x9 Detected padding

  %LC-3-SANTAANA: Santa Ana Asic: Line card instance 0, Serial Channel A (slot 2), Error
  Status 0x0

  %LC-3-IOTIMEOUT: RP CI-MUX FPGA read timeout (Slot 2, Serial Channel 0)
  ```

  Conditions: This symptom is observed once every 20 hours on a Cisco 7304 that has a CC-PA that runs firmware revision 1.40.

  Workaround: There is no workaround.

- CSCsg70929

  Symptoms: A 4-port OC-3 ATM line card (ESR-4OC3-ATM) may not restart properly on a Cisco 10000 series that has a PRE-2.

  Conditions: This symptom is observed only when the router boots while the MTU of the interface on the ESR-4OC3-ATM is different from the default MTU. The symptom does not occur if you change the default MTU of the interface after the router has booted.

  Workaround: Disable the **mtu** *bytes* interface configuration command and restart the ESR-4OC3-ATM.

- CSCsg71200

  Symptoms: During dynamic VLAN class modifications, the queueing policy inheritance fails. This situation causes traffic to be dropped.

  Conditions: This symptom is observed on a Cisco 10000 series that has a hierarchical queueing policy for VLAN classes and a flat shape for the class default. When the VLAN class modifications occur that shift the matching subinterfaces to the class default, then back to the original VLAN class, and then to another VLAN class, the child queues are not created, causing traffic to drop.

  Workaround: Remove and re-attach the hierarchical queueing policy.

- CSCsg71247

  Symptoms: Non-Priority Queuing (PQ) traffic in a class default in a QoS policy that includes the **match vlan** command is not dequeued during oversubscription of the PQ class.

  Conditions: This symptom is observed on a Cisco 10000 series only when there are multiple VLAN classes and when there are child queueing policies in the class default and the VLAN classes. The PQ policer takes the interface bandwidth as reference, causing policing to occur at the wrong rates and starvation of non-PQ child classes in the class default. The symptom does not occur for child classes in a VLAN class.

  Workaround: There is no workaround.

- CSCsg71400

  Symptoms: Traffic stops matching to a child policy.

Conditions: This symptom is observed on a Cisco 10000 series when an interface has a hierarchical policy defined on a PVC, when you remove the child policy, and when you re-attach the child policy to the parent policy of the hierarchical policy. In this situation, the traffic no longer matches to the child policy.

Workaround: Detach the hierarchical policy from the PVC, modify the child policy, and re-attach the hierarchical policy to the PVC.

- CSCsg71674

  Symptoms: T1 interfaces flap intermittently, causing input, CRC, frame, and abort errors to be generated.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(28)SB4.

  Workaround: There is no workaround.

- CSCsg72950

  Symptoms: Temperature alarms on a Cisco 10000 series PRE-3 assert at lower ambient temperatures than necessary.

  Conditions: This symptom may occur in an operating environment in which the ambient temperature is in the low 30s (degrees Celsius).

  Workaround: You can reprogram the temperature alarm thresholds. The recommended thresholds are:

  ```
  inlet minor: 41 C
  inlet major: 51 C
  inlet critical: 73 C
  outlet minor: 48 C
  outlet major: 58 C
  outlet critical: 85 C
  ```

- CSCsg73099

  Symptoms: When a client attempts to establish an IP session by using an IP assignment from the DHCP server of an Intelligent Service Gateway (ISG), the IP session may not be established.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when the following conditions are present:

  – The ISG is configured to initiate an IP session upon receipt of the first IP packet that does not have an IP session already, that is, the **initiator unclassified mac-address** or **initiator unclassified ip** command is enabled.

  – The IP session client receives its IP assignment from the DHCP server of the ISG and this DHCP server functions as a stand-alone DHCP server (that is, the IP assignment occurs without the influence of an ISG user and/or service profile).

  Workaround: In addition to or instead of the **initiator unclassified mac-address** or **initiator unclassified ip** command, enter the **initiator dhcp class-aware** command on the client-facing interface.

- CSCsg75132

  Symptoms: When the standby PRE comes up, the following error message is generated on the console of the active PRE:

  ```
  REDUNDANCY-3-IPC: cannot open standby port session in use
  ```

Conditions: This symptom is observed on a Cisco 10000 series that has dual PRE engines that function in ISSU, RPR+, or SSO mode.

Workaround: There is no workaround.

Further Problem Description: The error message indicates that some of the Entity MIB information such as standby PRE version, standby flash information, and standby EEPROM data has failed to synchronize to the active PRE.

- CSCsg75968

  Symptoms: When you enter the **clear counters** command, a Cisco 7304 that has an NSE-150 may crash and generate a TLB exception.

  Conditions: This symptom is observed when the Cisco 7304 is configured with 500 VRFs on an PA-A6 port adapter, when 250 VRFs are active, and when you perform a soft OIR for the PA-A6 and then enter the **clear counters** command.

  Workaround: There is no workaround.

- CSCsg76626

  Symptoms: A counter may indicate double values and packets are punted from the PXF engine to the RP and then dropped.

  Conditions: This symptom is observed on a Cisco 7304 when you apply an ACL deny statement on the egress interface.

  Workaround: There is no workaround.

- CSCsg76845

  Symptoms: Traffic loss, framing errors, CRC errors, input errors, and abort errors may occur on DS1 interfaces after an APS switchover occurs because a line card has reset.

  Conditions: This symptom is observed on the Cisco 10000 series that has a 1-port channelized OC-12 line card that is configured for channelized T3 traffic and MR-APS. The framing, CRC, input, and abort errors may occur even when traffic is not flowing.

  Workaround: There is no workaround.

- CSCsg76929

  Symptoms: The PXF engine of a Cisco 10000 series may crash.

  Conditions: This symptom is observed rarely on a Cisco 10000 series when MLP is configured and when member links flap frequently.

  Workaround: There is no workaround.

- CSCsg77139

  Symptoms: After you have reloaded a router, VRF routes disappear.

  Conditions: This symptom is observed when you reload a router the processes a heavy traffic flow.

  Workaround: Enter the **clear ip route vrf** *vrf-name* command.

  Alternate Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface from which the VRF routes have disappeared.

- CSCsg77753

  Symptoms: A router that has an hierarchical policy on an ATM VC may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7206VXR that is configured with an NPE-G1 but may be platform-independent.

Workaround: There is no workaround.

- CSCsg78469

  Symptoms: A Cisco 10000 series may generate a "SW_CORRUPTION" error message when a service of the ISG Layer 4 Redirect feature is removed from a session in a broadband aggregation (BBA) configuration.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an Intelligent Service Gateway (ISG) when a service of the ISG Layer 4 Redirect feature is removed via the configuration of a service policy.

  Workaround: There is no workaround.

- CSCsg79415

  Symptoms: After you have deleted a VLAN class from a bi-level policer policy in the ingress direction, class-default traffic is not aggregately policed by the parent policer that is defined for the default class.

  Conditions: This symptom is observed on a Cisco 10000 series that has a VLAN class with a child policer policy and a class default also with a child policy when you first attach the policy to an interface and then delete the VLAN class from the policy.

  Workaround: There is no workaround.

- CSCsg79638

  Symptoms: The PXF engine of a Cisco 10000 series may crash.

  Conditions: This symptom is observed rarely on a Cisco 10000 series when MLP is configured and when member links flap frequently.

  Workaround: There is no workaround.

- CSCsg81545

  Symptoms: A router may crash when you attach a Frame Relay map class to a subinterface that has already a map class attached or when you remove the DLCI from a Frame Relay subinterface that still has a map class attached.

  Conditions: These symptoms are observed on a Cisco 7200 series.

  Workaround: Remove the existing map class from the subinterface before you attach a new map class or remove the DLCI.

- CSCsg81678

  Symptoms: The aggregate values of the scheduler may be incorrectly updated for high-speed links. This situation may cause delay before policy maps take effect.

  Conditions: This symptom is observed on a Cisco 10000 series under rare circumstances with high-speed links such as 100 Mbps and Gigabit Ethernet links for which a parent shaper is configured.

  Workaround: There is no workaround.

- CSCsg81708

  Symptoms: Traffic drops occur when packets with a size of 64 bytes are being processed.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2.

  Workaround: There is no workaround.

- CSCsg82134

  Symptoms: When a line card failover occurs on a router that has redundant 4-port channelized T3 half-height line cards (ESR-HH-4CT3 line cards), the following error message and a traceback may be generated:

  ```
  %C10KHHCT3-4-LINECARDFAILOVER: LC Y-Cable cutover from subslot 4/1 due to freedm xmt
  partial packet fifo underrun error
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for failover protection through Y-cables when you initiate a line card failover by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on one of the ESR-HH-4CT3 line cards or by entering the **hw-module subslot** *slot-number/subslot-number* **reset** command for one of the ESR-HH-4CT3 line cards.

  Workaround: There is no workaround.

  Further Problem Description: Because of this caveat, the "xmt partial packet error" indication is currently not enabled to initiate an automatic line card failover on a router with redundant ESR-HH-4CT3 line cards. The error message is currently for information only.

  By nature, a line card failover may produce erroneous error indications on the line card. Further investigations have lead to the belief that the line card software is reading invalid error register information just after a failover occurs, producing an erroneous error message. Error indication registers should be cleared by the line card software following any line card failover before reading these registers again for valid error indications.

  When this caveats is resolved, the "xmt partial packet error" indication will be enabled as one of the mechanisms for an automatic line card failover.

- CSCsg85690

  Symptoms: When a policy map is unconfigured from a Fast EtherChannel (FEC) interface, a Cisco 7304 may crash and generate an "ALIGN-1-FATAL" error message without a traceback.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that is configured with 250 VRFs on the FEC interface. In addition, the Cisco 7304 is configured with 250 Frame Relay links and 250 dot1q VRFs. The symptom occurs while traffic is flowing through the FEC interface.

  Workaround: There is no workaround.

- CSCsg86230

  Symptoms: A router may crash when the execution of the **show policy-map** command is at the -More- prompt via one connection while the policy map is being modified or deleted via another connection.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-3 but may not be limited to this platform.

  Workaround: There is no workaround.

- CSCsg88356

  Symptoms: A ping between a CE router that is configured for ATM and another CE router that is configured for Ethernet may fail over an AToM tunnel when the **interworking ethernet** command is enabled on a connected PE router.

  Conditions: This symptom is observed on a Cisco 7200 series that functions as a PE router and may occur because of a timing issue. The symptom may not be platform-specific.

  Workaround: Do not enter the **interworking ethernet** command on the PE router. Rather, enter the **interworking ip** command.

- CSCsg88965

  Symptoms: When you first remove the **encapsulation frame-relay** command from a serial interface and then attempt to copy the startup configuration to the running configuration, a Cisco 7304 may crash and generate the following error message:

  ```
  Data Bus Error exception, CPU signal 10, PC = 0x40A24800.
  ```

  Conditions: This symptom is observed on a Cisco 7304 with an NSE-100 that has 250 Frame Relay, 250 Fast EtherChannel, and 250 dot1q VRFs while traffic is flowing through all these VRFs. QoS is configured on the core-facing interfaces of the Cisco 7304 and on the connected PE routers.

  Workaround: There is no workaround.

- CSCsg89189

  Symptoms: A router may reload when you enter the **show subscriber session detailed** command while sessions are being modified.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG).

  Workaround: Do not enter the **show subscriber session detailed** command while sessions are being modified.

- CSCsg90571

  Symptoms: On a Cisco 7200 series with an NPE-G1, channelized T3 links may flap. On a Cisco 7200 series with an NPE-G2, the serial interface may become wedged without the interface output queue being full.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(31)SB2 and that is configured with a 2-port multichannel T3 port adapter (PA-MC-2T3+).

  Workaround: There is no workaround.

- CSCsg95072

  Symptoms: The **show atm vc** command may be missing VCs.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB or a rebuild of Release 12.2(31)SB when at least one ATM line card is installed and VCs are configured.

  Workaround: You can display the ATM VC information by using a more specific command: enter the **show atm vc interface atm** *card/subcard/port* command.

  Further Problem Description: The missing VCs tend to be from select ATM subinterfaces.

- CSCsg97961

  Symptoms: A router may crash when you configure it with a high number of PPP over Ethernet over VLAN (PPPoEoVLAN) sessions that are spread over hundreds of VLAN subinterfaces.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2 or PRE-3.

  Workaround: There is no workaround.

- CSCsh07031

  Symptoms: L2TP connectivity may not function across the native Gigabit Ethernet interface of an NPE-G2.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(31)SB2 when EIGRP is configured as the routing protocol.

  Workaround: There is no workaround.

- CSCsh13947

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

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

  Workaround: There is no workaround.

TCP/IP Host-Mode Services

- CSCsd54305

  Symptoms: BGP sessions that are established between two route reflectors (RRs) flap continuously because TCP times out for keepalives.

  Conditions: This symptom is observed on a Cisco router that functions as an RR in an MPLS VPN Interautonomous System (InterAS) scenario and occurs when the RR receives VPNv4 prefixes from a PE router. In this situation, the BGP session between the RR and the second RR flaps.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCek54185

  Symptoms: When you add Variable Bit Rate (VBR) traffic shaping parameters to active PPPoA sessions, a Cisco 10000 series may crash and generate the following error message:

  ```
  %ERR-1-GT64120 (PCI-1)
  ```

  Conditions: This symptom is observed when PPPoA sessions without VBR are in the process of coming up while you add VBR traffic shaping parameters.

  Workaround: Wait until the sessions are completely up and then add VBR traffic shaping parameters.

- CSCek63810

  Symptoms: A Cisco 10000 series may run out of memory after a number of ATM port flaps have occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with 28,000 PPPoA Point-to-Point Termination and Aggregation (PTA) sessions. Each time that the ATM ports that carry the sessions flap and in this process remain down long enough for the sessions to time-out, more memory is lost.

  Workaround: There is no workaround.

- CSCsd06110

  Symptoms: A router may exhaust its I/O memory.

  Conditions: This symptom is observed on a Cisco router when you clear 10,000 tunnels on which about 45,000 PPP sessions are established. The symptom occurs only under extreme stress situations.

  Workaround: Clear the tunnels and sessions in stages.

- CSCsd95533

  Symptoms: PPP packets are dropped and the Network Control Programs (NCPs) are not negotiated.

  Conditions: This symptom is observed when you force a DHCP renewal of a lease for a DHCP client on a virtual-template interface.

  Workaround: Delete and reconfigure the virtual-template interface.

- CSCse19768

  Symptoms: A Cisco router crashes when you enter the **compress predictor** command to configure Predictor software compression.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100. However, the symptom is platform-independent.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur for Limpel Zif Stac (LZS) software compression.

- CSCse79790

  Symptoms: When PPPoE Relay is configured, only one session comes up successfully. All successive sessions fail. The initiation of more sessions brings down the existing sessions. If there are active sessions that are already existing (not necessarily PPPoE Relay sessions), the initiation of new PPPoE Relay sessions tears down all the sessions.

  Conditions: These symptoms are observed on a Cisco router that functions in a Virtual Private Dialup Network (VPDN). The symptom occurs only for PPPoE Relay sessions and not for normal sessions.

  Workaround: There is no workaround.

- CSCse86612

  Symptoms: A router that functions as an L2TP LNS for remote-end customer PCs that function as LACs crashes during normal operation.

  Conditions: This symptom is observed on a Cisco router that functions as a LNS in a Virtual Private Dialup Network (VPDN) and that runs Cisco IOS Release 12.2(28)SB2 or Release 12.4(8).

  Workaround: There is no workaround.

- CSCsg56725

  Symptoms: When you enter **terminate-from hostname** *host-name* command to terminate L2TP tunnels, some L2TP tunnels are terminated in the wrong VPDN group while other L2TP tunnels on the same host are terminated in the correct VPDN group.

  Conditions: This symptom is observed on a Cisco 7206VXR that has an NPE-G1 and that runs Cisco IOS Release 12.2SB and occurs only during the first two or three minutes after the router has booted. After that period, the symptom no longer occurs. Note that the symptom is platform-independent.

  Workaround: To prevent the symptom from occurring, enter the **no aaa accounting system guarantee-first** command on the router before you reload the router. Doing so enables the tunnels to be terminated in the correct VPDN groups.

  After the symptom has occurred, clear each of the affected tunnels by entering the **clear vpdn tunnel id** *local-id* command. Then, after the tunnels have been re-established, you should be able to terminate them in the correct VPDN groups.

- CSCsg76884

  Symptoms: A PRE may crash.

  Conditions: This symptom is observed rarely on a Cisco 10000 series that is configured for PPP and occurs when many serial links flap.

  Workaround: There is no workaround.

- CSCsg79798

  Symptoms: The number of SHDB handles for PPP, SIP, and a Cisco CallManager may increase considerably on the active RP. In this situation, when a switchover occurs, many interfaces may end up in the up/down state.

  Conditions: This symptom is observed on a Cisco router that has dual RPs in a situation in which 1000 serial interfaces flap every 12 seconds for 10 hours.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(31)SB2

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(31)SB. This section describes only severity 1, severity 2, and select severity 3 caveats.

Note All caveats that are resolved in Cisco IOS Release 12.2(28)SB and Release 12.2(28)SB1 through Release 12.2(28)SB5 are also resolved in Release 12.2(31)SB2. To improve the usability of the release notes documentation, these resolved caveats are documented only in the sections for Release 12.2(28)SB1 through Release 12.2(28)SB5 and are not repeated in the "Resolved Caveats—Cisco IOS Release 12.2(31)SB2" section.

Basic System Services

- 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.

- CSCek43597

  Symptoms: A memory leak may occur on a router that is configured with 11,000 PPPoA and PPPoEoA sessions.

  Conditions: This symptom is observed when AAA HA is used to synchronize the authorization data from the standby RP to the active RP and when a RADIUS server is used.

  Workaround: Use local authentication. If this is not an option, there is no workaround.

- CSCek58968

  Symptoms: A RADIUS packet that is sent to a RADIUS server may contain a corrupted attribute.

  Conditions: This symptom is observed on a Cisco router that is configured for AAA and that has the **radius-server vsa send authentication** command enabled.

Workaround: Disable the **radius-server vsa send authentication** command.

- CSCin98160

  Symptoms: Sessions are not properly synchronized from the active RP to the standby RP after an HA switchover has occurred.

  Conditions: This symptom is observed on a Cisco router that has the **no aaa new-model** command enabled.

  Workaround: Configure local authentication and enter the **aaa new-model** command. If this is not an option, there is no workaround.

- CSCin99788

  Symptoms: An “%AAA-3-ACCT_LOW_MEM_TRASH” error message is generated when a low-memory condition occurs. When this situation occurs, a memory leak may occur in AAA data.

  Conditions: This symptom is observed when an interface flaps and causes a very large number of sessions to go down simultaneously, in turn generating a very large number of accounting stop records. In this situation, the I/O memory may be held for a long time when accounting records are send and when an AAA server is slow or unreachable.

  Workaround: There is no workaround.

- CSCsc73699

  Symptoms: A router that is configured for NetFlow v9 may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(25)S4 or Release 12.2(27)SBC1 when the configuration is modified while the router actively exports flows. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- 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.

- CSCse30963

  Symptoms: The following error message and a traceback may be generated on a Cisco 7200 series:

  ```
  %SYS-3-MGDTIMER: Uninitialized timer, set_exptime, timer
  ```

  Conditions: This symptom is observed when you perform an OIR of a channelized port adapter, when you configure a channel group on channelized interfaces of a channelized port adapter, or when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on any interface.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur on a Cisco 7200 series that has an NPE-G2.

- CSCse36870

  Symptoms: An ISG crashes when a Change of Authorization (CoA) is issued upon account logon.

Conditions: This symptom is observed on a Cisco router that functions as an ISG while the password attribute is sent in the Account-Logon request.

Workaround: There is no workaround.

- CSCse68964

  Symptoms: When a PTA session is created with a traffic classifier (TC) service, the Parent-Session-ID attribute of the accounting packets of the TC service on the ISG does not match the Acct-Session-Id of the parent session after 16^2 (that is, 000000EE) Acct-Session-Ids have been used.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG and that is configured with QinQ subinterfaces over which PTA sessions are established.

  Workaround: There is no workaround.

- CSCse78879

  Symptoms: The **radius-server attribute 31 remote-id** command does not function. The expected value of attribute 31 in a RADIUS Access-Request and Accounting-Request is only the value of the remote ID. However, attribute 31 may contain the host name, domain name, subinterface and description, in addition to the remote ID.

  Conditions: This symptom is observed on a Cisco router that functions as a NAS and that has the **radius-server attribute 31 remote-id** command enabled.

  Workaround: There is no workaround.

- CSCsf07847

  Symptoms: Specifically-crafted CDP packets may cause a router to allocate and hold extra memory. Exploitation of this behavior by sending multiple specifically-crafted CDP packets may cause memory allocation problems on the router.

  Conditions: This symptom is observed on a Cisco router when the header length of the CDP packet is shorter than the predefined header length (which is 4 bytes) and when the router runs a Cisco IOS software image that integrates the fix for CSCse85200.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse85200. Cisco IOS software releases that are not listed in the “First Fixed-in Version” field at this location are not affected.

  Workaround: Disable CDP on interfaces where CDP is not required.

  Further Problem Description: Because CDP is a Layer-2 protocol, the symptom can only be triggered by routers that reside on the same network segment.

- CSCsf11826

  Symptoms: When AAA and High Availability (HA) are configured, “SHDB handles” are not properly released when the **no aaa new-model** command is enabled on the router. For each session (that is, each PPPoA or PPPoE session) that comes up, a new “SHDB handle” is allocated. However, when the session goes down, the “AAA HA code” fails to release the handle. This situation causes the router to use up all valid handle names, and, after that has occurred, to either generate tracebacks for each session that is created or to crash.

  Conditions: This symptom is observed for each session that calls the “AAA HA code” to handle redundancy.

  Workaround: Enable the **aaa new-model** command and configure local authentication. If this is not an option, there is no workaround.

- CSCsf23387

  Symptoms: After a network event such as an HA switchover or an interface failure has occurred, information for all PPP sessions may be lost, causing the router to send RADIUS account-start messages for all PPP sessions and causing the RADIUS server to be severely stressed.

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

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat relieves the impact on the RADIUS server by enabling you to limit the maximum number of outstanding active RADIUS accounting request via the AAA accounting throttling command that is introduced below. This command is introduced not only for HA configurations but for general AAA operations.

  radius-server throttle accounting *requests*

  The *requests* argument limits the number of pending accounting start/stop requests that are sent by the router to the RADIUS server. For example, if the *requests* argument has a value of 25, the number of pending accounting start/stop requests (without a RADIUS acknowledgement) is at maximum 25. If a new accounting request must be processed and the router has already sent 25 requests, the router will attempt to send the new accounting request after a “timeout”. The request will be delayed with the value in seconds that is entered in the *timeout* argument of the following command:

  radius-server timeout *timeout*

  The router does not discard these accounting request if they time-out. Only if the router has actually attempted to send the accounting request to the RADIUS server and has retransmitted it three times, the accounting request may be discarded. Note that the retransmit default is three but can be modified through the **radius-server retry** *retries* command.

  If an accounting request is throttled, statistics are not impacted in any way. The statistics are updated only if an accounting request is sent to the RADIUS server, not when it is being throttled. You can check for the active accounting requests by entering the following command:

  show aaa servers

  Note that accounting has no impact on call setups. From the perspective of a client, it is a “send-and-forget” situation. The success or failure of accounting does not impact the actual session.

- CSCsf29098

  Symptoms: When you perform an OIR of a POS port adapter, a TLB Exception error may occur and the router may reset.

  Conditions: This symptom is observed on a Cisco router that has a POS port adapter with an interface that functions as an MPLS link in an AToM configuration when the POS interface has the **mpls ip** command enabled.

  Workaround: First disable the **mpls ip** command on the POS interface, then remove the AToM (Xconnect) configuration from the interface, and then perform an OIR of the POS port adapter.

- 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**.

- CSCsg48183

  Symptoms: A router may unexpectedly send an ARP request from all its active interfaces to the nexthop of the network of an SNMP server.

  Conditions: This symptom is observed on a Cisco router that has the **snmp-server host** command enabled after any of the following actions occur:

  - You reload the router.
  - A switchover of the active RP occurs.
  - You enter the **redundancy force-switchover main-cpu** command.

  Workaround: There is no workaround.

- CSCsg77508

  Symptoms: The parent session Accounting STOP record is missing RADIUS attributes 42,43, 47 and 48.

  Conditions: This symptom is observed on a Cisco router that is configured to terminate a PPP over Ethernet over L2TP session when you apply a service policy to the session. The symptom occurs only when the session is configured with at least one traffic classification with per-flow accounting.

  When the PPP over Ethernet client is terminated, the RADIUS attributes 42, 43, 47 and 48 are missing from the parent session Accounting STOP record.

  Workaround: There is no workaround.

EXEC and Configuration Parser

- CSCsc76550

  Symptoms: The RP may crash with a watchdog timeout error for the IP input process.

  Conditions: This symptom is observed on a Cisco router when you delete a subinterface that processes traffic.

  Workaround: Shut down the subinterface before you delete the subinterface.

IBM Connectivity

- CSCsf28840

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

  There are workarounds available for this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml.

Interfaces and Bridging

- CSCek43732

  Symptoms: All packets are dropped from a 1-port OC-3/STM-1 POS port adapter (PA-POS-1OC3) or 2-port OC-3/STM-1 POS port adapter (PA-POS-2OC3) that is configured for CBWFQ.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1. However, the symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCek46082

  Symptoms: A router may crash when one of its multipoint interface enters the up state.

  Conditions: This symptom is observed on a Cisco 7200 series when the multipoint interfaces are configured for AAL5SNAP encapsulation via a virtual template and occurs only when the **debug atm event** command is enabled.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCed28542

  Symptoms: A router that is configured for PAT may generate the following error message and traceback while reporting slowness in the network:

  ```
  %SYS-2-INTSCHED: 'may_suspend' at level 3
  -Process= "IP NAT Ager", ipl= 3, pid= 118
  -Traceback= 80507F58 81310988 80CC14F8 80CD4F80 80CBAD30 80CBAD90 81321684 80CBB048
  80504118 805085E0
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(4)T and that has a high number (more than 2500) of NAT entries. The symptom is not release-specific.

  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.

- CSCek48132

  Symptoms: A router that is configured for HA may crash shortly after a switchover has occurred. When this situation occurs, "%TCP-2-INVALIDTCB" error messages are generated.

  Conditions: This symptom is observed on a Cisco router that has many interfaces (1600) that are connected to BGP neighbors when some peers are configured for NSR and others for NSF. The higher the number of interfaces on the router, the more likely it is that the symptom occurs.

  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.

- 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.

- 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.

- 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.

- CSCse67198

  Symptoms: A router may hang when you send a VRF ping to an outside NAT address of a directly-connected router.

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

  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.

- 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.

- 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.

- CSCsg27697

  Symptoms: When an RP switchover occurs or when a standby RP resets, the standby RP may enter a loop in which it reboots continuously because of a BEM error.

  Conditions: This symptom is observed on a Cisco router that has the **router rip** and **address-family ipv4** commands enabled but that does not have a **network** command as part of the address-family configuration.

  Workaround: Disable the **router rip** command.

Miscellaneous

- 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.

- CSCec54103

  Symptoms: When the ifStackStatus object of an inverse multiplexing over ATM (IMA) interface is polled with an “snmpwalk,” an endless loop may occur.

  Conditions: This symptom is observed on a Cisco router that is configured with an 8-port ATM Inverse MUX E1 or T1 port adapter (PA-A3-8E1IMA or PA-A3-8T1IMA).

  Workaround: There is no workaround.

- CSCef09119

  Symptoms: CPUHOG tracebacks may be generated when you bring up 30,000 PPPoE sessions and then remove an input policy map from a virtual template on a broadband PTA.

Conditions: This symptom is observed on a Cisco router that functions as a broadband PTA and that is configured with 31,500 ATM subinterfaces, an input policy map, an output policy map with an CBWFQ policy, and 128,000 queues.

Workaround: There is no workaround.

- CSCeg83467

  Symptoms: A router crashes when the encapsulation is changed from AAL5SNAP to AAL0.

  Conditions: This symptom is observed when the encapsulation is changed on a private virtual circuit (PVC).

  Workaround: Do not configure AAL0.

- CSCeh86935

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

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

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

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

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

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

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

- CSCei39688

  Symptoms: When a CEF initialization failure occurs, an ATM PVC that is configured for OAM may not pass traffic even though the PVC link status is up:

  ```
  Router#show ip interface brief | include ATM
  ATM3/0/0                unassigned      YES manual up       up
  ATM3/0/0.100            unassigned      YES unset  up       up
  ATM3/0/0.300            10.1.1.1        YES manual up       up
  ATM3/0/0.999            unassigned      YES unset  up       up


  Router#show cef interface brief | include ATM
  ATM3/0/0                     unassigned      up      dCEF
  ATM3/0/0.100                 unassigned      down    dCEF
  ```

```
ATM3/0/0.300                    10.1.1.1        down    dCEF
ATM3/0/0.999                    unassigned      down    dCEF

Router#show ip cef | include 10.1.1.
10.1.1.0/30     attached             ATM3/0/0.300
```

When CEF fails to initialize the ATM PVC, atm3/0/0.300, no /32 receive entries are created. Traffic that is destined for the IP address of the subinterface is dropped.

Conditions: This symptom is observed on a Cisco router and occurs only when PAM is configured on the PVC.

Workaround: To prevent the symptom from occurring, do not configure OAM on the PVC. When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected ATM subinterface. After the workaround has been applied, the output of the **show ip cef** command shows the following:

```
Router#show ip cef | include 10.1.1.
10.1.1.0/30     attached             ATM3/0/0.300
10.1.1.0/32     receive
10.1.1.1/32     receive
10.1.1.3/32     receive
```

- 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.

- CSCej78971

  Symptoms: Unicast Reverse Path Forwarding (uRPF) does not function for a PPP subscriber when the **ip portbundle** command is enabled on the interface that carries the subscriber session. The following example shows a configuration in which the symptom occurs:

  ```
  interface Serial3/0
   ip vrf forwarding vrf1
   ip address x.x.x.x y.y.y.y
   ip verify unicast source reachable-via rx  <***** uRPF enabled
   encapsulation ppp
   service-policy type control ipsub-auth
  ```

  In the above-mentioned example, if the **ip portbundle** command is enabled in the “ipsub-auth” policy map, the source address of the interface that carries the subscriber traffic is changed to one of the IP addresses of the ISG, and the reverse-path check causes the traffic to be dropped.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG.

  Workaround: Disable the uRPF.

- CSCek34307

  Symptoms: After a service policy is removed from the virtual template, the same policy is not automatically removed from the virtual-access interface.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB or Release 12.2(27)SBC.

Workaround: Clear the virtual-access interface.

- 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.

- CSCek38382

  Symptoms: The standby PRE-2 crashes because of a debug exception, and the standby PRE-2 console shows the following error messages and traceback before the crash occurs:

  ```
  %SYS-2-ASSERTION_FAILED: Assertion failed: "(*parents_ptr)->coll_magic ==
  COLL_MAGIC_VAL"
  -Process= "Deferred Adj Background", ipl= 0, pid= 167
  -Traceback= 6050CA04 604AA1B4 60362364 60362510 603630A4 6035B67C 60360598 60FFAB30
  60FF54A0 60FF5578
  ```

  ```
  %Software-forced reload
  ```

  Conditions: This symptom is observed on a Cisco 10000 series after an ATM line card is reset.

  Workaround: There is no workaround.

- CSCek38430

  Symptoms: The standby PRE reloads unexpectedly.

  Conditions: This symptom is observed on a Cisco 10000 series when either of the following events occur:

  - Multiple users simultaneously add and delete service policies.
  - Multiple users periodically enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on an ATM subinterface. For example, the users enter the commands with intervals of 5 to 10 seconds during a period of 2 or 3 minutes.

  Workaround: There is no workaround.

- CSCek39134

  Symptoms: During an HA configuration synchronization a router may generate the following error message:

  ```
  %UTIL-3-TREE: Data structure error--attempt to reference an uninitialized wavl tree
  ```

  Conditions: This symptom is observed rarely on a Cisco router when auto-discovery packets are received by the router during the initialization phase after an HA switchover has occurred or after the router has reloaded for the first time.

  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.

- CSCek40657

  Symptoms: A PTA router may crash when you download a configuration with a class map, policy map, and PVC range to a point-to-point interface.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PTA router.

  Workaround: There is no workaround.

- CSCek41883

  Symptoms: An RP may hang when PPPoX sessions are brought up.

  Conditions: This symptom is observed after an HA switchovers has occurred.

  Workaround: There is no workaround.

- CSCek42581

  Symptoms: A router crashes when you modify a police in the parent policy map.

  Conditions: This symptom is observed on a Cisco 10000 series when you first remove a class with a police that is configured under a parent policy map and then re-apply the same class or any other class with a police to the parent policy map.

  Workaround: Remove the parent policy map, reconfigure the parent policy map, and the re-attach the parent policy map.

- CSCek44373

  Symptoms: The standby RP may generate "%SYS-2-MALLOCFAIL: Memory allocation" failures and may or may not reset repeatedly.

  Conditions: These symptoms are typically observed in highly scaled configurations that consist, for example, of many BGP peers or PPPOA sessions. The symptoms occur during the SSO configuration-synchronization phase and bulk-synchronization phase when the standby RP comes online, during the configuration of the router, after a switchover, or when peer interfaces and/or routing neighbors flap. The symptom is more likely to occur on an RP that does not contain so much physical I/O memory and/or operates at a relatively slow CPU speed.

  Workaround: Scale down the configuration, or reduce the number of BGP peers or PPPOA sessions. If the peer neighbors or interfaces flap, determine the root cause, and correct the flapping problem.

- CSCek45299

  Symptoms: A policer configuration may not be removable from a policy map.

  Conditions: This symptom is observed on a Cisco 10000 series when policy-map classes have a priority level configured.

  Possible Workaround: Remove the policy map, reconfigure the policy map, and then re-attach the policy map.

- CSCek45570

  Symptoms: ISSU negotiation or a bulk synchronization fails, causing the standby RP to reload.

  Conditions: This symptom is observed on a Cisco router that is configured for HA when the ISSU client or DHCP client is not present on the peer.

  Workaround: There is no workaround.

- CSCek46135

  Symptoms: There is no interception when a time-based ACL rule is inactive.

  Conditions: This symptom is observed on a Cisco 10000 series that has the Lawful Intercept feature enabled.

Workaround: There is no workaround.

- CSCek48136

  Symptoms: A router may crash when QoS policy changes occur for a large number of VCs.

  Conditions: This symptom is observed on a Cisco router when the QoS changes are made via an automated script.

  Workaround: Modify the VCs manually, one by one.

- CSCek48457

  Symptoms: A Cisco 10000 series crashes when a scaled MFR configuration is loaded.

  Conditions: This symptom is observed when you load the scaled MFR configuration by using TFTP via the **copy tftp running-config** command.

  Workaround: There is no workaround.

- CSCek48575

  Symptoms: A router may crash when you first enter the **ip portbundle** command for PPPoE sessions in a port-bundle host key (PBHK) configuration and when you then change an ACL.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG and that has a configuration such as the following:

  ```
  ip portbundle
   length 3
   match access-list 103
   source Loopback2
  ```

  Workaround: There is no workaround.

- 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.

- CSCek52071

  Symptoms: A Cisco 7200 series may crash when you configure an IPv6 address on an interface.

  Conditions: This symptom is observed on a Cisco 7200 series that has the Lawful Intercept feature enabled.

  Workaround: There is no workaround.

- CSCek53084

  Symptoms: Attachment circuit (AC) and AToM clients show up as compatible while they have no peer on the other side.

  Conditions: This symptom is observed on a Cisco router that is configured for In-Service Software Upgrade (ISSU) when you downgrade from Cisco IOS Release 12.2(31)SB to Cisco IOS Release 12.2(28)SB or one of it’s rebuilds.

  Workaround: There is no workaround.

- CSCek53559

  Symptoms: A router may reload after receiving a malformed UDP packet on port 67.

Conditions: This symptom is observed on a Cisco router that functions as an DHCP server.

Workaround: There is no workaround.

- CSCek54106

  Symptoms: When you convert a non-queueing policy map to a queueing policy map and attach it to interfaces that do not support queuing, the QoS policy is removed from the interfaces and existing sessions.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Convert the non-queueing policy map to a queueing policy map before you apply it to interfaces or bring up sessions.

- CSCek54768

  Symptoms: E1 interfaces may go down when a line card is reset or removed even when the line card has APS enabled and an APS cutover is triggered. The interfaces do come back up within a few seconds.

  Conditions: This symptom is observed on a Cisco 10000 series that has a pair of 4-port channelized OC-3 line cards that are configured for SR-APS. The line cards are configured with E1 interfaces under either SONET or SDH.

  Workaround: Enter the **force** command in APS group configuration mode on both the router on which the line card is reset or removed and on the router at the far end to ensure that the line card that is reset or removed does not receive or transmit the active traffic.

  Note that the chances of the symptom occurring may be reduced when the line card that is reset or removed is not the active line card.

  Further Problem Description: This symptom occurs only when a line card is reset or removed, not when an APS switchover is triggered by a fiber cable that is removed.

  The symptom occurs because of a change in the E1 clock source that may occur when the line card is reset or removed and that causes alarms to be received. The symptom is more likely to occur when the line card has a large configuration and when the E1 interfaces are set to “clock source line.”

- CSCek55284

  Symptoms: When you upgrade the Cisco IOS software image from Cisco IOS Release 12.2(28)SB3 to Cisco IOS Release 12.2(31)SB by entering the **issu loadversion** command, the standby RP remains in the RPR mode, preventing the upgrade from proceeding.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCek55726

  Symptoms: When you reload a Cisco 10000 series that has dual PREs, the standby PRE may crash during the boot process and may or may not generate a traceback.

  Conditions: This symptom is observed on a Cisco 10000 series that has a large configuration when the standby PRE and primary PRE are out of synchronization while you enter the **reload** command.

  Workaround: There is no workaround.

- CSCek55946

  Symptoms: A Cisco 7304 series NPE-G100 may hang.

  Conditions: This symptom is observed when a cache exception occurs, which is a very rare event.

  Workaround: There is no workaround.

- CSCek56055

  Symptoms: When an IP session that was initiated by DHCP goes down, the session cannot be reconnected until the lease expires for the client.

  Conditions: This symptom is observed on a Cisco Intelligent Service Gateway (ISG) when an idle-timeout occurs, when the ISG reloads, or when a client logs off without releasing the IP address.

  Workaround: Manually clear the DHCP binding or just wait until the lease expires.

- CSCek56415

  Symptoms: The Hierarchal Queuing Framework (HQF) is not removed after you have removed a service policy.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 and that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCek56991

  Symptoms: A Cisco 7200 series may send a corrupted packet via a 2-port T3 serial, enhanced port adapter (PA-2T3+). The rate of corrupted packets is very low.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2SB, Release 12.4T, or Release 12.4(4)XD3 and occurs when the router functions under high stress conditions such as a high CPU load and an oversubscribed interface of the PA-2T3+.

  Workaround: Avoid a high CPU load and oversubscription of the interface of the PA-2T3+.

- CSCek57646

  Symptoms: On a Cisco 10000 series, tracebacks and an error message that is related to the link index may be generated, and MLPoATM links continue to flap. The error message is similar to the following:

  ```
  %GENERAL-3-EREVENT: ttcm_add_mlp_member: 1926 No free link index available in
  Virtual-Access15
  ```

  Conditions: This symptom is observed when a member link of an MLPoATM bundle is modified.

  Workaround: There is no workaround.

- 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.

- CSCek59190

  Symptoms: When you reload a Cisco 10000 series, tracebacks are generated when the router comes back up.

  Conditions: This symptom is observed when the router has dual PREs that function in SSO mode and a 4-port channelized STM-1/OC-3 line card that is configured for Multi-Router APS (MR-APS).

  Workaround: There is no workaround.

- CSCek59985

  Symptoms: A traceback may be generated during the “fetch_interface_drop_stats_clrable” process on a Cisco 10000 series.

Conditions: This symptom is observed when you enter the **clear pxf interface** command for an inactive multilink interface.

Workaround: Enter the **clear pxf interface** command only when the multilink interface is active.

- CSCek60629

  Symptoms: A Cisco 10000 series may crash because of an address error (that is, a load or instruction fetch exception) when multiple combined command-line interface (CLI) changes are made.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for RPR+ when you attempt to make multiple policy map changes on a PVC that has a small number of active sessions with a moderate amount of downstream traffic.

  Workaround: There is no workaround.

- CSCek62271

  Symptoms: The output of the **show ip subscriber** command does not show the sessions.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) and occurs for IP session with a static IP address that are connected via Layer 2.

  Workaround: Do not enter the **show ip subscriber** command. Rather, enter the **show ip subscriber mac** command.

- CSCek63748

  Symptoms: When the **debug ip subscriber event** or **debug ip subscriber all** command is enabled and when a client attempts to establish an IP session, the Cisco Intelligent Service Gateway (ISG) may crash.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG under the following conditions:

  - The ISG is configured to initiate an IP session upon receipt of the first IP packet that does not have an IP session already, that is, the **initiator unclassified mac-address** or **initiator unclassified ip** command is enabled.
  - There is a DHCP relay between ISG and the client.
  - The IP session client receives its IP assignment from the DHCP server of the ISG and this DHCP server functions as a stand-alone DHCP server (that is, the IP assignment occurs without the influence of an ISG user and/or service profile).

  Workaround: Disable the **debug ip subscriber event** or **debug ip subscriber all** command.

- CSCin99827

  Symptoms: An RP may crash when PPP sessions with service policies are removed. If the router is configured with a standby RP, a switchover may occur. Then, if more PPP sessions are removed, the newly active RP may crash. These symptoms may also occur when you enter the **no policy-map** command for a policy map that is attached as a service policy to many PPP sessions.

  Conditions: These symptoms are more likely to occur with a large number of sessions (tens of thousands or more) and when the session are removed at a high rate (hundreds per second).

  Workaround: There is no workaround.

  Further Problem Description: The symptoms are caused by a race condition when internal processes, such as statistics updates, may attempt to modify data that are related to service policies that are being removed.

- CSCir00590

  Symptoms: VCs may enter an inactive state, preventing sessions from coming up over the VCs.

Conditions: This symptom is observed on a Cisco 10000 series when you perform an OIR of the line card on which the VC are configured after at least one HA switchover has occurred.

Workaround: Reload the router.

- CSCir00613

  Symptoms: An ATM line card may reset after when an SSO switchover occurs.

  Conditions: This symptom is observed on a Cisco 10000 series when an SSO switchover occurs while there are 32,000 active PPP over ATM (PPPoA) sessions.

  Workaround: There is no workaround.

- CSCsa92748

  Symptoms: A Network Processing Engine G1 (NPE-G1) may restart unexpectedly and report the following message:

  ```
  Last reset from watchdog reset
  ```

  Conditions: This symptom is observed only on Cisco 7200 and Cisco 7301 series routers that are configured with an NPE-G1 Network Processing Engine.

  Workaround: There is no workaround.

- CSCsb01284

  Symptoms: Incorrect police percent conversions occur in the second and third level of a policy.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2SB but may also occur on other platforms and in other releases.

  Workaround: There is no workaround.

- CSCsb12598

  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.

- 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.

- CSCsb71154

  Symptoms: When a VC that is configured under a VP goes down, PPPoE sessions can still be established over the VC.

  Conditions: This symptom is observed on a Cisco 10000 series after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the main interface or after you have reloaded the router.

  Workaround: There is no workaround.

- CSCsc14052

  Symptoms: A Cisco 10000 series may crash and generate one of the following error messages:

  ```
  PXF DMA Error - Command Packet Handle Out of Range
  ```

  or:

  ```
  PXF DMA - Small Free Packet Handle Access Out of Range
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that processes L2TP traffic and that has a heavy CPU load.

  Workaround: There is no workaround.

- CSCsc44272

  Symptoms: When a Cisco 7304 has a configuration with more than 65,536 ACEs, some of the counters do not increment correctly.

  Conditions: This symptom is observed when the entire ACE configuration is greater than 65,336 ACEs.

  Workaround: There is no workaround. Do not configure more than 65,536 ACEs.

- CSCsd35159

  Symptoms: Alignment errors may occur when you detach a shaping service policy from a QinQ subinterface.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsd45936

  Symptoms: When a two-level hierarchical policy map in which the parent level has only a class default is already attached to an interface and when you configure a policer for both the parent and child levels, either of the following symptoms may occur:

  - When the child policy map is removed from the class default of the parent policy map, the traffic policing rate does not properly reflect the parent policer rate.
  - When the child policy map is attached to the class default of parent policy map, the traffic policing rate does not properly reflect the child policer rate.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB.

  Workaround: After the child policy is removed from or attached to the parent policy map, detach the policy map from the interface and re-attach it to the interface.

- 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.

- CSCsd60687

  Symptoms: When an RPR switchover occurs, a router may generate CPUGHOG messages or may crash because of a watchdog timeout.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB or Release 12.2SR.

  Workaround: There is no workaround.

- CSCsd65283

  Symptoms: A router may crash when you enter the **connect** command.

  Conditions: This symptom is observed when one of the VCs that is being configured in the **connect** command is down.

  Workaround: Ensure that both VCs are up when you enter the **connect** command.

- CSCsd65497

  Symptoms: When a GRE IP tunnel is configured between a CE router and a PE router and is added to the VRF table, the IP address of the tunnel on the PE router is not reachable from the CE router although the IP address of the tunnel on the CE router is reachable from the PE router.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that functions as a PE router.

  Workaround: There is no workaround.

- CSCsd82991

  Symptoms: A router crashes when you enter the **ip rtp header compression** command on a serial interface that has a service policy attached.

  Conditions: This symptom is observed on a Cisco router and occurs only when a routing protocol, such as EIGRP, has been configured.

  Workaround: There is no workaround.

- CSCsd85852

  Symptoms: When a PVC is shut down on the remote side, the PVC subinterface on a router transitions from the down state to the up state within one second, but then remains in the down state after the down retry timers expire.

  Conditions: This symptom is observed on a Cisco router that is configured for Operation, Administration, and Maintenance (OAM) and Dynamic Bandwidth Selection (DBS).

  Workaround: There is no workaround.

- CSCsd85990

  Symptoms: Multilink class 0 is used for all outgoing packets, regardless of which encapsulation sequence is configured for a queue.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for Multiclass MLP (MC-MLP) with one member link and occurs after the PXF engine is reloaded.

  Workaround: 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.

- CSCsd95631

  Symptoms: When you enter the **show atm vp** command for ATM VPs, a negative number of data VCs is displayed, which does not represent the actual number of VCs per VP.

  Conditions: This symptom is observed on a Cisco 10008 that runs Cisco IOS Release 12.3(7)XI. However, the symptom is not platform-specific, nor release-specific.

  Workaround: There is no workaround.

- 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.

- CSCse01989

  Symptoms: When you apply a channel group to a Gigabit Ethernet interface that has the **negotiation auto** command enabled, the **negotiation auto** command is unexpectedly enabled on the port-channel interface. This situation causes a synchronization failure on the standby RP, in turn, causing the standby RP to reset.

  Conditions: This symptom is observed on a Cisco router that has redundant RPs in an HA configuration.

  Workaround: Manually remove the auto-negotiation configuration from the port-channel interface by entering the **no negotiation auto** command.

- CSCse08652

  Symptoms: When you configure MVPN over an MLPoATM interface, multiple PXF crashes may occur.

  Conditions: This symptom is observed on a Cisco 10000 series when you first enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the MLPoATM interface and then enter the **show pxf cpu queue** *interface* command on the MLPoATM interface. After these commands, the PXF crashes start. This situation may cause the boot flash to be fully consumed.

  Workaround: There is no workaround.

- CSCse11078

  Symptoms: When you enter the **aps force** or **aps manual** command on a Cisco 10000 series router that has interfaces that are configured for Multi-Router APS (MR-APS), the standby PRE may not properly reflect the MR-APS state of the interfaces.

  Conditions: This symptom is observed in a configuration with two Cisco 10000 series routers that are configured with dual PREs that function in SSO mode.

  Workaround: There is no workaround.

- CSCse13674

  Symptoms: A session does not receive an IP address from the VRF pool.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when a VRF is configured in an automatic activation service with Transparent Auto-Logon (TAL).

  Workaround: Do not configure a VRF in an automatic activation service.

- CSCse15417

  Symptoms: When about 40,000 sessions are created, a Cisco router that functions as an Intelligent Service Gateway (ISG) may reload.

  Conditions: This symptom is observed only when auto services are used to bring up the sessions and when a low-memory condition occurs.

  Workaround: Do not use auto services to bring up the sessions.

- 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.

- CSCse23190

  Symptoms: After a forced SSO switchover has occurred, the next hop in the routing table becomes 0.0.0.0.

  Conditions: This symptom is observed on a Cisco router that is configured with PPPoEoA sessions.

  Workaround: There is no workaround.

- CSCse23232

  Symptoms: When a virtual template or user profile contains a service policy with class maps, the router may send not one but a number of RADIUS accounting-request packets for each PPPoE or PPPoEeoA session. The number of RADIUS accounting-request packets equals the number of class maps in the service policy. Each accounting-request packet has its own unique "acct- session-id."

  Conditions: This symptom is observed on a Cisco router that is configured with a QoS policy.

  Workaround: There is no workaround.

- 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.

Workaround: There is no workaround.

- CSCse25431

  Symptoms: A LAC may generate an "HQF_WARN_HQF_OVERSUBSCRIPTION_DETECTED" error message when it is oversubscribed with a high number of sessions. The LAC may crash when it is severely oversubscribed.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a LAC when you scale PPPoEoQinQ sessions with QoS configured and when you oversubscribe to a very high rate. The oversubscription is configured on a subinterface via an MQC policy that is enabled through the **shape average percent** *percent* command.

  Workaround: Do not configure the oversubscription factor above the supported factor of 50:1.

- CSCse28714

  Symptoms: Removing and re-attaching a policy to a subinterface may fail because of cleanup issues.

  Conditions: This symptom is observed on a Cisco 10000 series when a hierarchical policy with PBR in the parent policy class-default class is applied to the session that is established on the subinterface.

  Workaround: There is no workaround.

- CSCse28795

  Symptoms: When a service policy is configured on an ATM main interface that has a PVC on a subinterface (the PVC does not have its own policy), an "%C10K_QOS_GENERAL-e-EREVENT" error message and traceback are generated when the PVC is recreated.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PE router in an MPLS network that has the following topology:

  ```
  CE1 -- PE1 -- P -- PE2 -- CE2
  ```

  Workaround: There is no workaround. However, the error message and traceback have no functional impact.

- CSCse31706

  Symptoms: A Lawful Intercept configuration improperly shows as part of an interface configuration.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCse32421

  Symptoms: A PXF buffer leak may occur when a Multilink PPP interface is shut down on the other side of a back-to-back configuration.

  Conditions: This symptom is observed on a Cisco 10000 series and is caused by packets that become stuck in the multilink bundle queue when the connected router crashes or is reloaded, or when a remote interface is shut down. When all links are removed from the multilink bundle, the packets are still queued up in the multilink bundle. Because there is no serial link to dequeue the packets, the packets remain in the queue.

  Workaround: There is no workaround.

- CSCse35684

  Symptoms: OSPF sessions do not come up at the Layer-3 level.

  Conditions: This symptom is observed when you perform an OIR of an ATM line card.

Workaround: Reload the affected line card.

- CSCse36785

  Symptoms: Packets that are switched via CEF to a service network with DHCP-based IP subscribers may be dropped at an ISG.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when both of the following conditions occur:

  - A subscriber sets the DHCP broadcast bit in a DHCP request to zero, as a Microsoft DHCP host typically does.
  - The subscriber connection occurs via Dynamic VPN selection, that is, the subscriber connects to the ISG via a global interface but the IP address is assigned by VPN services that are selected by the subscriber.

  Workaround: If the DHCP client is a router that runs a Cisco IOS software image, enter the **ip dhcp-client broadcast** command on router. If the DHCP client runs Microsoft software, there is no workaround.

- CSCse36890

  Symptoms: Multicast packets that traverse GRE tunnels over a Gigabit EtherChannel (GEC) bundle interface may be dropped because of multicast RPF failures.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Do not use a GEC bundle. Rather, configure the GRE tunnels on regular GE interfaces.

- 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.

- CSCse41596

  Symptoms: A Cisco router does not update the IP address of a RADIUS proxy session, and the RADIUS proxy session is terminated after the IP address timer expires.

  Conditions: This symptom is observed only when the router functions both as an Intelligent Service Gateway (ISG) and as a DHCP server.

  Workaround: There is no workaround.

- CSCse42494

  Symptoms: A router crashes when it has more than 65,536 L2TP sessions in a multiple-hop configuration. At a multiple-hop router, an L2TP session is created inbound and outbound for each user session. This means that the number 65,536 is exceeded when more than 32,768 sessions are traversing the tunnel.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Configure less than 32,768 user sessions (half of 65,536).

- CSCse43394

  Symptoms: When traffic is sent through 250 LFI over Frame Relay interfaces, the other side does not receive any traffic. Also, no packets are dequeued on the priority queue (PQ).

Conditions: This symptom is observed on a Cisco 10000 series.

Workaround: There is no workaround.

- CSCse43461

  Symptoms: The VC state remains down after and interface flap occurs on an MFR interface that has Frame Relay end-to-end keepalive (EEK) configured. The EEK state remains down although the MFR interface is up.

  Conditions: This symptom is observed on a Cisco 10000 series when the MFR interface has the following Frame Relay class map configured:

  ```
  map-class frame-relay eek
   frame-relay end-to-end keepalive mode bidirectional
  ```

  and also

  ```
  frame-relay multilink bandwidth-class c
  ```

  The symptom occurs when you enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the MFR interface.

  Workaround: To prevent the symptom form occurring, enter the **frame-relay end-to-end keepalive error-threshold send 3** command in the Frame Relay class map. The default value is 2.

  When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface at the other side of the MFR interface.

- CSCse44067

  Symptoms: A Cisco 7304 that has an ATM-IMA port adapter may crash.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 when you configure an ATM-IMA subinterface with an IP address.

  Workaround: There is no workaround.

- CSCse45054

  Symptoms: When there is bidirectional traffic over PPPoE sessions over an Auto VC and you perform an OIR of the line card that processes this traffic, a few VCs are not cleared from the line card when the idle timeout is reached. This situation prevents sessions from coming up on the affected VCs.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Perform a second OIR of the line card.

- CSCse47905

  Symptoms: When an IP session that was initiated by DHCP goes down, the session cannot be reconnected until the lease expires for the client.

  Conditions: This symptom is observed on a Cisco Intelligent Service Gateway (ISG) when an idle-timeout occurs, when the ISG reloads, or when a client logs off without releasing the IP address.

  Workaround: Manually clear the DHCP binding or just wait until the lease expires.

- CSCse48657

  Symptoms: The active RP unexpectedly resets the standby RP.

  Conditions: This symptom is observed when you configure an Embedded Event Manager (EEM) policy and when the policy file is only available on the active RP and not on the standby RP.

Workaround: Before you configure the EEM policy, copy the policy file to the standby RP at the same location as the policy file is located on the active RP.

- CSCse49912

  Symptoms: When end-to-end Frame Relay fragmentation (FRF.12) is configured for a Multilink Frame Relay (MFR) (FRF.16.1) bundle, the Frame Relay configuration may become lost and packets with a size that is smaller than the fragmentation size cannot pass.

  Conditions: This symptom is observed on a Cisco 10000 series when end-to-end Frame Relay fragmentation is configured on the main interface, that is, not via a Frame Relay map class and occurs when the interface flaps.

  The following configuration provides an example of an end-to-end Frame Relay configuration that is applied directly to the main interface:

```
interface MFR4
 description c10k FRF.16 test
 ip address 10.0.0.1 255.255.255.252
 load-interval 30
 no arp frame-relay
 frame-relay multilink bandwidth-class c 3
 frame-relay fragment 80 end-to-end
 frame-relay interface-dlci 17
```

  Workaround: Reconfigure end-to-end Frame Relay fragmentation by entering the following sequence of commands:

  no frame-relay fragment *fragment-size* **end-to-end**

  frame-relay fragment *fragment-size* **end-to-end**

  Alternate Workaround: Apply end-to-end Frame Relay fragmentation via a Frame Relay map class.

- CSCse50992

  Symptoms: Traffic that matches a prepaid service that consists of a traffic class and a volume monitor is matched with a default traffic class instead, causing the traffic to pass unbilled.

  Conditions: This symptom is observed on a Cisco 10000 series when traffic is sent continuously after reauthorization has occurred.

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

- CSCse51043

  Symptoms: A router may generate tracebacks and may crash when you bring up a Gigabit Ethernet (GE) interface.

  Conditions: This symptom is observed when you first shut down the GE interface and then bring it up with a large number of IPoQinQ VLANs.

  Workaround: There is no workaround.

- CSCse53212

  Symptoms: When a switchover occurs, a traceback may be generated on a router that is configured with a large number of PPPoE sessions, and the router may crash.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS and LDP and occurs only when the number of PPPoE sessions reaches beyond 30,000. However, the traceback (without a crash) may occur even for 500 PPPoE sessions.

Workaround: There is no workaround.

- CSCse53669

  Symptoms: You may not be able to change the Dynamic Bandwidth Sharing (DBS) parameters for some create on-demand PVCs, and the DBS parameters for some PVCs may change when they are not supposed to change.

  Conditions: This symptom is observed on a Cisco 10000 series you enter the **dbs enable** or **no dbs enable** command for a range of ATM PVCs after VCs have been brought up. The symptom does not occur for VCs that are brought up for the first time after the DBS configuration has changed.

  Workaround: This workaround applies only to a VC that does not process traffic for a while. The purpose of this workaround is to bring down a VC connection in order to change the DBS parameters.

  Enter the **dbs enable** or **no dbs enable** command, as needed. Then, enter the **pvc-in-range** *vpi vci* command for a particular VC and enter the **idle-timeout** *seconds* command with a non-zero value for the *seconds* argument to enable the session to expire when there is no traffic on the VC. Check the output of the **show atm vc** *vcd* command until the VC goes down or disappears. Remove the **idle-timeout** *seconds* command or restore this command to its former value.

- CSCse57312

  Symptoms: The MQC output policer does not add the L2 header as part of its calculation.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs only for multicast traffic on Ethernet and ATM interfaces.

  Workaround: There is no workaround.

- CSCse57808

  Symptoms: An eBGP session on the MFR interface continues to flap if one of the links in the MFR bundle is down while the bundle is up.

  Conditions: This symptom is observed only when Frame Relay EEK is enabled on the MFR interface. The symptom does not occur when Frame Relay EEK is not configured on the MFR interface.

  Workaround: Ensure that all links in the bundle are up. If you must bring down one link, do not shut the link down, but remove it from the bundle.

- CSCse59096

  Symptoms: Traffic with large packets cannot be fragmented through an MFR bundle that is configured for end-to-end Frame Relay fragmentation (FRF.12) after you have removed a service policy from the MFR interface.

  Conditions: This symptom is observed on a Cisco 10000 series when an output policy map is first added and then removed. Packets with sizes that are smaller than the fragmentation size can still be transmitted.

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

- CSCse60008

  Symptoms: A router crashes when a packet with a PPP header that includes a bad IP version is sent over an MLP link.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for SSO.

  Workaround: There is no workaround.

- CSCse61320

  Symptoms: A PRE-2 may crash when remove the last **match vlan** class-map configuration command from the last class map in a policy that is attached to an interface.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Remove the class map by entering the **no class-map** *class-map-name* command.

- CSCse65884

  Symptoms: The **atm pvp** *vpi* **l2transport** command may disappear from the configuration.

  Conditions: This symptom is observed after you have reloaded the router.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, reconfigure the command.

- CSCse65966

  Symptoms: Low traffic throughput occurs when you detach a VLAN policy from an interface.

  Conditions: This symptom is observed on a Cisco 10000 series when the VLAN policy that is being detached has a child policy under a default class for non-VLAN group members.

  Workaround: There is no workaround.

- CSCse66782

  Symptoms: When RSA keys are generated at first, both the active and the standby RP receive the RSA key. However, after an HA RP switchover has occurred, the new standby RP no longer has the RSA key. When you reset the standby RP, the RSA key is not synchronized to the standby RP either. After another HA switchover has occurred, both the active and the standby RP have lost the RSA key, which then must be regenerated.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB. However, the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCse68044

  Symptoms: The user name that is sent to accounting and authorization servers is blank, causing prepaid services and billing to fail.

  Conditions: This symptom is observed on a Cisco router when ISG is configured to perform Transparent Auto-Logon (TAL) for PPP sessions and when there is no authentication configured on the virtual template that is used for the PPP sessions.

  Workaround: There is no workaround.

- CSCse68788

  Symptoms: The console hangs and there is no response to any CLI commands.

  Conditions: This symptom is observed on a Cisco 10000 series that has a large broadband configuration with 40,000 PTS sessions, each one with a QoS service policy. The symptom occurs when active sessions are disconnected at a high rate (200 disconnections per second).

  Workaround: Slow down the session disconnection rate.

  Further Problem Description: The symptom does not occur when sessions without a QoS service policy are disconnected.

- CSCse70667

  Symptoms: A router crashes during an attempt to access the interface policy-map statistics.

Conditions: This symptom is observed on a Cisco 10000 series that is configured with invalid policy maps that have VLAN classes with invalid filter types.

Workaround: There is no workaround.

- CSCse72235

  Symptoms: A Cisco 7200 series may crash because of an address error with corrupted program counter at “pc=0xAFACEFAD.” This precise value is repeated in the traceback and in the “EPC,” “BadVaddr,” and “ra” registers. The crash may be preceded by a “%SYS-2-GETBUF: Bad getbuffer” error message.

  Conditions: This symptom is observed on a Cisco 7200 VXR router that has an NPE-G1 and that runs Cisco IOS Release 12.2(28)SB2. The router is configured as a LAC with PPPoA and MPLS fragmentation for packets that travel from a PPPoA interface through an L2TP tunnel to an interface that is configured for MPLS.

  Workaround: Disable MPLS.

  Alternate Workaround: Disable fragmentation.

- CSCse75238

  Symptoms: A router may crash when the service-policy information of a session is displayed.

  Conditions: This symptom is observed when tens of thousands of sessions are established on a PTA router that has a service-policy instance for each session via a policy map on a virtual template.

  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.

- CSCse77804

  Symptoms: When you downgrade the Cisco IOS software image from Cisco IOS Release 12.2(33)SB to Release 12.2(28)SB, the download fails.

  Conditions: This symptom is observed on a Cisco 10000 series that has redundant PREs (PRE A and PRE B) and that is configured for ISSU when the following sequence of events occurs:

  1. The active PRE is switched over from PRE A to PRE B.
  2. The **loadversion** command is issued from PRE B, which is the active PRE.

  Workaround: There is no workaround.

  Further Problem Description: The symptom does not occur when PRE A is the active PRE and when the **loadversion** command is issued from PRE A.

- 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.

- CSCse78987

  Symptoms: The PXF engine may crash because of an invalid sequence of DMA commands.

  Conditions: This symptom is observed on a Cisco 10000 series when a multicast packet is replicated on an interface on which an Intelligent Service Gateway (ISG) session is established.

  Workaround: There is no workaround.

- CSCse79166

  Symptoms: Policing may not function on a Cisco 10000 series.

  Conditions: This symptom is observed when a parent policy map has a **police** command enabled and when a child policy map has a set action.

  Workaround: Do not configure a simple set action in the child policy map. Rather, configure a **police** command with a set action in the child policy map.

- 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.

- CSCse81528

  Symptoms: A newly active 4-port channelized T3 half-height line card (ESR-HH-4CT3) in subslot 0 may reload when a previously active ESR-HH-4CT3 is unplugged from subslot 1.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs only in a configuration with a redundant Y-cable in which subslot 1 is the active ESR-HH-4CT3.

  Workaround: There is no workaround.

- CSCse83989

  Symptoms: When you reset or insert a line card while traffic is flowing, the line card may reset continuously.

  Conditions: This symptom is observed on a Cisco 10000 series that has a 1-port channelized OC-12 line card and a 4-port channelized OC-3 line card.

  Workaround: Stop the traffic that is destined for the line card before you reset or insert the line card.

- 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.

- CSCse87221

  Symptoms: Tracebacks are generated during an SSO switchover.

Conditions: This symptom is observed on a Cisco router when you enter the **redundancy force-failover main-cpu** command.

Workaround: There is no workaround.

- CSCse87499

  Symptoms: A platform that is configured for Cisco IOS Redundancy Facility (RF) may reload unexpectedly.

  Conditions: This symptom is observed when an RF client fails while the standby RP attempts to transition to the hot standby state.

  WorkAround: There is no workaround.

- CSCse88338

  Symptoms: A router crashes when you first enter the **clear subscriber session all** command and then enter the **show ip subscriber dangling** *number-of-seconds* command.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG while processing traffic.

  Workaround: Do not enter the **show ip subscriber dangling** *number-of-seconds* command or the **clear ip subscriber dangling** *number-of-seconds* command.

- 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) switchover 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.

- 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.

- CSCse91989

  Symptoms: ISSU Client 2063 (ISSU DHCPC) that is only present in Cisco IOS Release 12.2(31)SB2 shows up as compatible in a release that does not support the client.

  Conditions: This symptom is observed when you downgrade from Cisco IOS Release 12.2(31)SB2 to a release that does not yet support the client.

  Workaround: There is no workaround.

- CSCse93327

  Symptoms: A Cisco 10000 series may crash when you modify a class map.

  Conditions: This symptom is observed when the QoS configuration is scaled to a high number of VLAN classes and when you attempt to delete a child class with a WRED configuration from a policy that is attached to a VLAN group class.

  Workaround: First, remove the WRED configuration from the class. Then, delete the class.

Alternate Workaround: Detach the service policy from the interface, delete the class, and then re-attach the service policy to the interface.

- CSCse93747

  Symptoms: When you configure QoS on an ATM PVC under a point-to-point subinterface, the router may not accept and save an output service policy when an input service policy is already present on the interface.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a PRE-2 or PRE-3.

  Workaround: First configure the output service policy and then configure the input service policy.

- CSCse94304

  Symptoms: A PRE crashes, and CPUHOG error messages are generated.

  Conditions: This symptom is observed on a Cisco 10000 series that functions in an MR-APS configuration with another Cisco 10000 series and that has MLP configured.

  Workaround: Disable MLP.

- CSCse94879

  Symptoms: When you upgrade from Cisco IOS Release 12.2(27)SBB5 to Release 12.2(27)SBB6 by using ISSU, a traffic interruption of about 30 seconds may occur on an OC-12 POS line card.

  Conditions: This symptom is observed on a Cisco 10000 series that has redundant PRE-2 processors and one or more OC-12 POS line cards. The symptom could also occur with other releases.

  Workaround: There is no workaround.

  Further Problem Description: The upgrade should reload the OC-12 POS line card but not reset the line card. Instead, an internal error occurs on the line card, causing the line card to crash. However, the line card automatically reboots and successfully recovers, and traffic resumes after about 30 seconds of interruption.

- CSCse95010

  Symptoms: For a bi-level policy that has the **shape percent** command enabled for the parent match-vlan class and that has the **bandwidth percent** command enabled for the child class, the bandwidth is not proper computed at the child class when the *percent* argument of the **shape percent** command of the parent match-vlan class exceeds the value 50, that is, the shaper rate is more than 50 percent.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Ensure that the *percent* argument of the **shape percent** command of the parent match-vlan class does not exceed the value 50.

  Further Problem Description: When the **bandwidth remaining percent** command is removed from the parent match-vlan class, the following error message is generated:

  Please remove bandwidth from the child policy and re-issue command.

  When you detach the parent policy from the main interface and re-attach it to the main interface, the child class miscomputes the bandwidth because it takes zero as reference rather than the shaper rate of the parent class.

- CSCse96084

  Symptoms: “Suspend/Activate service-policy” messages flood the console when there are thousands of sessions hosted on the router.

Conditions: This symptom is observed on a Cisco 10000 series when the sessions come up or go down.

Workaround: Disable console logging on the router.

Further Problem Description: The messages are internal messages that should not appear on the console.

- CSCse97283

  Symptoms: ARPs may be lost. This situation may cause adjacencies to go down, which, in turn, may cause peer routers to stop responding.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs only when buffer memory is extremely congested for one minute or more. For example, extreme congestion occurs when the "low buffer hdl drop(s)" counter in the output of the **show pxf cpu stat drop 1** increments at a rate that is equal to the incoming ARP traffic rate.

  Workaround: There is no workaround.

- CSCse99137

  Symptoms: A Cisco router that functions as an Intelligent Service Gateway (ISG) returns the wrong value in Cisco Vendor Specific Attribute (VSA) 250 (ssg-account-info) in a RADIUS packet.

  Conditions: This symptom is observed when the ISG responds to a service query from a Cisco Subscriber Edge Services Manager (SESM) or service provider portal server.

  Workaround: There is no workaround.

- CSCsf05044

  Symptoms: In a very large-scale MLPP configuration, that is, more than 300 MLP bundles, when a PRE-2 HA switchover occurs on a Cisco 10000 series, the following error message and/or a traceback may be generated on the connected Cisco 10000 series at the far end:

  ```
  ttcm_add_mlp_member: unable to install mlp link
  ```

  Conditions: This symptom is observed during the renegotiation of the links and line protocol of the interfaces and bundles.

  Workaround: There is no workaround.

- CSCsf05685

  Symptoms: A router that functions as a DHCP server and DHCP relay may fail to issue or renew a lease.

  Conditions: This symptom is observed after a class name is uploaded onto the DHCP server, which causes the parameters of DHCP-initiated sessions for an ISG to be changed.

  Workaround: There is no workaround.

- CSCsf08208

  Symptoms: The username attribute is not present in the accounting stop records.

  Conditions: This symptom is observed when a PPP session is brought up with Transparent Auto logon (TAL).

  Workaround: There is no workaround.

- CSCsf10896

  Symptoms: The parent session ID attribute is not present in the accounting records for prepaid services.

Conditions: This symptom is observed on a Cisco router that functions as an ISG when accounting is enabled for any prepaid service.

Workaround: There is no workaround.

- CSCsf12056

  Symptoms: A LAC does not tap upstream packets via the CISCO-TAP2-MIB.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a LAC and that has the Lawful Intercept feature enabled.

  Workaround: There is no workaround.

- CSCsf12124

  Symptoms: The policer conform, exceed, and violate counters (both packets and bytes) in the output of the **show policy-map interface** command may stop incrementing and freeze at a certain value.

  When this situation occurs, usually, the bytes counters freeze first, and then, after some time, the packet counters freeze too. This situation may also cause the "policer drop-rate bps counter" to become stuck at zero because the "policer drop-rate bps counter" is based on changes in the bytes counters.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG and occurs when the counters are very large, that is, at or very near their limits.

  Temporary Workaround: Remove and then re-apply the policy map on the interface to reset the counters to zero.

- CSCsf13802

  Symptoms: eBGP sessions may go down when they are established on MFR subinterfaces with several VPNs between a Cisco 10000 series that functions as a PE router and a Cisco 7200 series that functions as a CE router.

  Conditions: This symptom is observed when the Cisco 10000 series has input and output service policies and Frame Relay fragmentation configured in a map class that is applied to DLCIs on the MFR subinterfaces. The symptom occurs while there is no traffic on the MFR link between the PE and CE routers.

  Workaround: Remove either the service policies or Frame Relay fragmentation from the map class.

- CSCsf15121

  Symptoms: Packets that are encapsulated via PPPoE and that are generated by a Cisco 10000 series and sent to a PPPoE client may take into account the padding of the incoming frame in the length field of the PPPoE header. This situation may cause problems for certain protocol stacks.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a LAC or PTA router and that terminates PPP over Ethernet over ATM (PPPoEoA), PPP over Ethernet over Ethernet (PPPoEoE), PPP over Ethernet over Queue in Queue (PPPoEoQinQ), or PPP over Ethernet over VLAN (PPPoEoVLAN) sessions. The incoming frames are Ethernet or PPPoEoA frames, which can be padded because of the 64-byte minimum frame size requirement of Ethernet.

  The symptom is caused by the fix for caveat CSCsd13298, which uses the full incoming frame size as the length field of the PPPoE header of the outgoing packet.

  A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd13298. 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.

- CSCsf15164

  Symptoms: When a PRE-2 crashes and when the router is configured with a redundant PRE-2, a "PCI Retry Expire" error may occur after the crashinfo file has been generated.

  Conditions: This symptom is observed on a Cisco 10000 series and may occur even when the redundant PRE is not booted but remains in ROMmon.

  Workaround: There is no workaround.

  Further Problem Description: Note that the "PCI Retry Expire" error is not the original cause for the crash, but is a secondary issue.

- CSCsf17039

  Symptoms: A router may crash when you configure On-Demand Address Pools (ODAP) with Dynamic Host Configuration Protocol (DHCP) and when the router that requests the address pool (subnet) runs out of available addresses.

  Conditions: This symptom is observed in an MPLS-VPN network when you configure ODAPs on virtual home gateways (VHGs) and provider edge (PE) routers.

  Workaround: There is no workaround.

- CSCsf24720

  Symptoms: The PXF engine may crash when tapping is enabled.

  Conditions: This symptom is observed on a Cisco 10000 series that has the Lawful Intercept feature enabled when a truncation of the padding of a packet occurs, causing the Lawful Intercept feature to generate a replica.

  Workaround: There is no workaround.

- CSCsf25920

  Symptoms: The line protocol for an MFR interface may be up and the DLCIs may be in the active state even though the LMI is down.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB and occurs for MFR interfaces.

  Workaround: There is no workaround.

- CSCsf25978

  Symptoms: By default, a Cisco 10000 series PRE-2 should police a priority class to 95 percent of the link bandwidth to prevent other queues from starving. However, the priority class may use up to 100 percent of the link bandwidth if no policer is configured.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB.

  Workaround: Configure a policer in the priority class.

- CSCsf27230

  Symptoms: When you configure a policy with WRED and shaping, random drops do not occur.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100.

  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 IISU. 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.

- CSCsf28159

  Symptoms: ISG accounting reports identical counter values for all services in the VSAs.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when the "accounting-list" is removed from the VSAs that are included in the request from the Cisco Subscriber Edge Services Manager (SESM).

  Workaround: Configure the SESM to include the "accounting-list" in the VSAs that are sent to the ISG.

- CSCsf28725

  Symptoms: The **match cos** command does not function when it is applied to a QoS policy in the output direction.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2 when the output policy map is configured on an interface that has an L2 VPN configuration.

  Workaround: There is no workaround.

- CSCsf30762

  Symptoms: When bidirectional traffic passes a 1-port Gigabit Ethernet half-height line card, the Gigabit Ethernet ingress and egress interface counters report zero packets/second and zero bits/second.

  Conditions: This symptom is observed on a Cisco 10000 series when there is a large number (at least 10,000) of interfaces and/or broadband sessions and when traffic is sent over the Gigabit Ethernet interface of a 1-port Gigabit Ethernet half-height line card.

  Workaround: There is no workaround.

- CSCsf96715

  Symptoms: The PXF engine may crash while a PPPoX session is established between a LAC and an LNS.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a LAC and that has a QoS configuration.

  Workaround: Disable the QoS configuration on the LAC.

- CSCsf98115

  Symptoms: AAA output counters for Tx bytes and octets remain zero or are incorrect for LAC sessions.

  Conditions: This symptom is observed on a Cisco 10000 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.

- CSCsg00072

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

  1. Symptom 1: The PXF engine may crash continuously.

     Condition 1: This symptom is observed on a Cisco 10000 series that has a PRE-2 and that is configured for LFI over ATM when IPCP is negotiated.

     Workaround 1: Disable the LFIoATM bundle interface.

  2. Symptom 2: Multilink PPP over ATM (MLPoA) member links may flap because of keepalive failures.

     Condition 2: This symptom is observed on a Cisco 10000 series that has a PRE-2 when keepalives are enabled on the bundle interface.

     Workaround 2: Disable keepalives on the bundle interface.

- CSCsg00438

  Symptoms: Some Cisco 10000 series line cards may become stuck.

  Conditions: This symptom is observed when the router functions in a redundant configuration and occurs after you have reloaded the router.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, power-cycle the affected line cards or perform an OIR of the affected line cards.

- CSCsg02980

  Symptoms: The CCM client holds up the Redundancy Framework (RF) progression.

  Conditions: This symptom is observed on a Cisco router that is configured for HA and PPP.

  Workaround: There is no workaround.

- CSCsg03916

  Symptoms: TACACS+ accounting on/off messages are not sent after a router has been reloaded.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for AAA and TACACS+ system accounting. The symptom may not be platform-specific.

  Workaround: There is no workaround.

- CSCsg09654

  Symptoms: After a switchover has occurred, “IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP” error messages are displayed on both the primary and standby RP, it takes while for the primary RP to come up, and the standby RP does not come up at all.

  Conditions: These symptoms are observed on a Cisco 7304 that has dual RPs that functions in SSO mode.

  Workaround: There is no workaround.

- CSCsg09825

  Symptoms: A Cisco 10000 series may crash when a PPPoE session is brought up.

  Conditions: This symptom is observed only when the VC over which the PPPoE session is brought up has both the **dbs enable** command and a queuing service policy enabled.

Workaround: Either disable the **dbs enable** command or remove the queuing service policy before the PPPoE session is brought up.

- CSCsg11718

  Symptoms: A VRF may become stuck in the "Delete Pending" state.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN and Half-Duplex VRF (HDVRF) when you delete the VRF and then associate it with an interface before it is completely deleted.

  Workaround: To ensure that the VRF is properly deleted, enter the **shutdown** interface configuration command on the interface with which the VRF is associated or remove the interface with which the VRF is associated.

- CSCsg12800

  Symptoms: A subscriber session setup fails when a VRF transfer is initiated at the start of the session.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG.

  Workaround: There is no workaround.

- CSCsg13086

  Symptoms: A router crashes when range PVCs are created on an Auto VC on a point-to-point subinterface.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCsg13118

  Symptoms: A Cisco 7304 crashes when you enter the **show warm-boot** command or **no warm-boot** command.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for warm reboot.

  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.

  Workaround: Remove the QoS configuration. If this is not an option, there is no workaround.

- CSCsg18289

  Symptoms: Applying a line loopback onto an ATM interface has no effect.

  Conditions: This symptom is observed on a Cisco 10000 series when you enter the **loopback line** command on an ATM interface. The output of the **show interfaces atm** command shows that "loopback set" and "loopback line" appear in the configuration. However, the "loop" LED on the line card does not illuminate either. Traffic through the interface continues uninterrupted.

Workaround: There is no workaround.

- CSCsg18894

  Symptoms: When you attempt to change or overwrite the **priority** command for a MQC priority queue, the command is rejected and the following error message is generated:

  ```
  priority not allowed in conjunction with queue-limit
  ```

  Conditions: This symptom is observed on a Cisco router that has the **queue-limit** command enabled in a MQC priority queue.

  Workaround: Remove the **queue-limit** command, modify the **priority** command, and then re-enter the **queue-limit** command.

- CSCsg19684

  Symptoms: A channel-group configuration on a physical interface is not removed when you perform an OIR of the port adapter on which the channel group is configured.

  Conditions: This symptom is observed on a cisco 7304 that is configured for Fast EtherChannel (FEC).

  Workaround: Enter the **no channel-group** *channel-number* command before you perform an OIR of the port adapter.

- CSCsg21425

  Symptoms: ACL entries that include L4 match criteria may not match properly.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2 and an ACL with eight or less rules when at least one rule is a “permit” rule that specifies L4 matching criteria.

  Workaround: Add a few dummy rules to the ACL to ensure that the ACL has more than eight rules. Doing so enables the L4 match criteria to match properly.

- CSCsg24343

  Symptoms: A Cisco 7304 may crash when LFIoATM configured on a PA-A3-OC3MM port adapter that is installed in a PA-CC and when traffic starts to flow over the ATM link.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100.

  Workaround: There is no workaround.

- CSCsg24451

  Symptoms: Some line cards may be reported as deactivated when the router boots.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB and usually occurs for Gigabit Ethernet or Fast Ethernet line cards.

  Workaround: Enter the **hw-mod subslot** *slot*/*subslot* **reset** command for each affected line card.

  Alternate Workaround: Reload the router again.

- CSCsg27043

  Symptoms: On a 7304 series Network Services Engine (NSE), the passing of packets from the PXF engine to the RP may freeze for a period from seconds to minutes. This situation causes the router to lose its routing protocol neighbors.

  Conditions: This symptom is observed rarely on a Cisco 7304 that runs Cisco IOS Release 12.2S or Release 12.2SB.

  Temporary Workaround: If the symptom occurs repeatedly, reloading the router may help.

- CSCsg29086

  Symptoms: An ISG may crash and generate the following error messages and a traceback:

  ```
  %ALIGN-1-FATAL: Corrupted program counter 17:47:38 ESTDST Thu Oct 5 2006 pc=0x0,
  ra=0x0, sp=0x6436AB80
  %ALIGN-1-FATAL: Corrupted program counter 17:47:38 ESTDST Thu Oct 5 2006 pc=0x0,
  ra=0x0, sp=0x6436AB80
  TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x0 -Traceback=
  ```

  Conditions: This symptom is observed on a Cisco router that function as an ISG and that is configured for Dynamic Host Configuration Protocol (DHCP).

  Workaround: There is no workaround.

- CSCsg29539

  Symptoms: In an MPLS core that carries EoMPLS traffic, an ingress PE router that has a TE tunnel to an egress PE router may stop sending EoMPLS traffic after the TE tunnel is rerouted across a different path in the MPLS core. When you enable the **debug mpls packet** command on the first P router in the topology, the debugs show that the EoMPLS packets enter with the wrong (that is, the old) TE tunnel label.

  Conditions: This symptom is observed on a Cisco 7304 that functions as a PE router and that runs Cisco IOS Release 12.2(28)SB or one of its rebuilds.

  Workaround: Clear the interface.

- CSCsg30757

  Symptoms: The following symptoms may occur for prepaid accounting:

  - There are no gigabit word attributes 52 and 53 for prepaid service, but when you enable the **debug radius** command, attributes 52 and 53 are shown for the parent session.
  - The prepaid service always sends the rollover counters in “I” and “O” as zero although the definitions are “I<HC>;<LC>” and “O<HC>;<LC>” in which HC indicates the rollover counter and LC indicates the lower 32 bit of the input and output octets counters.

  The following is part of the debugs and shows “I0;1963039136” and “O0;1963039136” and no attributes 52 and 53 (“gigaword rollover counters”) although the amount of traffic over this service has exceeded the gigaword and has rolled over once already:

  ```
  RADIUS:   Cisco AVpair       [1]   36  "parent-session-id=0A0A440200000003"
  RADIUS:  Vendor, Cisco       [26]  21
  RADIUS:   ssg-control-info   [253] 15  "I0;1963039136"
  RADIUS:  Vendor, Cisco       [26]  21
  RADIUS:   ssg-control-info   [253] 15  "O0;1963039136"
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB and that is configured with a prepaid service policy.

  Workaround: There is no workaround.

- CSCsg31202

  Symptoms: A Cisco 7304 with an NSE-100 may crash and generate the following error message:

  ```
  Unexpected exception, CPU signal 10, PC = 0x4008B2EC
  ```

  Conditions: This symptom is observed very rarely when the router is configured with an input policy that marks incoming IP traffic on one interface and then uses this information for classification on an output policy on another interface.

  Workaround: There is no workaround.

- CSCsg32638

  Symptoms: The default MIR value for the priority queue is incorrectly set to the CIR value for the priority queue, causing latency and throughput problems on the priority queue.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB.

  Workaround: There is no workaround.

- CSCsg35305

  Symptoms: A Cisco router that functions as an Intelligent Service Gateway (ISG) reloads when you enter the **show database** command.

  Conditions: This symptom is observed when existing sessions are in the process of being disconnected and when you enter the **show database** command for these sessions.

  Workaround: Do not enter the **show database** command for sessions that are in the process of being disconnected.

- CSCsg36725

  Symptoms: A memory leak and memory exhaustion may occur when QoS policies are updated on 40,000 sessions.

  Conditions: This symptom is observed on a Cisco 10000 series but may also affect other platforms.

  Workaround: There is no workaround.

- CSCsg37423

  Symptoms: The output of the **show l2tun session l2tp** command does not include interface information.

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

  Workaround: There is no workaround.

- CSCsg40949

  Symptoms: The PXF engine of a Cisco 10000 series may crash.

  Conditions: This symptom is observed rarely on a Cisco 10000 series when MLP is configured and when member links flap frequently.

  Workaround: There is no workaround.

- CSCsg43177

  Symptoms: Memory loss may occur when a microcode reload is being processed.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured as a 6PE router and occurs because of unnecessary allocation of IPv6 adjacencies.

  Workaround: There is no workaround.

- CSCsg45686

  Symptoms: The following warning message may be generated when PPPoX sessions are being established:

  ```
  %C10K_BBA_SESSION-4-WRN2EVENT: Temporarily unable to add session to VC session list
  ```

  Although this warning message is a low-priority message, the number of messages may be quite high when a large number of sessions is being established.

  Conditions: This symptom is observed on a Cisco 10000 series when an operation fails during the attempt to establish a session.

Workaround: There is no workaround. However, the error message has no system impact, and the session is established during a next attempt.

- CSCsg47298

  Symptoms: When an IP session is deleted, a Cisco 10000 series may reload because of an exception.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG and that has both PBHK and police features installed for an IP session.

  Workaround: Do not configure police features for an IP session when PBHK is already configured for that IP session.

- CSCsg47598

  Symptoms: Unrecoverable memory loss may occur when you reload part or all of a configuration that has QoS policies that are active. In a large-scale configuration (that is, a configuration with many active policies), this situation may cause memory exhaustion.

  When the symptom occurs, the output of the **show processes memory sorted holding** command shows a reduction in free memory between reloads of the same configuration with QoS policies that are active.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCsg47601

  Symptoms: When a Cisco router that functions as an Intelligent Service Gateway (ISG) also functions as a DHCP server or relay, the DHCP client may receive the wrong IP address or does not receive an IP address at all.

  Conditions: This symptom is observed when an IP DHCP session is terminated to a VRF via a service profile that is automatically activated during the session creation and when more than one auto service is configured in the user profile.

  Workaround: Configure only one auto service (VRF Service) in the user profile.

- CSCsg50778

  Symptoms: A Cisco 10000 series crashes because of memory violations when you attempt to set the 4096th tap.

  Conditions: This symptom is observed on a Cisco 10000 series that has the Lawful Intercept feature enabled.

  Workaround: The maximum number of taps is 4095. Do not set more than 4095 taps.

- CSCsg59671

  Symptoms: Accounting record counters are incorrect when accounting is applied to an IP Interface session.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an Intelligent Service Gateway (ISG) and occurs only for IP Interface sessions.

  Workaround: There is no workaround.

- CSCsg60122

  Symptoms: A Cisco 10000 series that functions as an Intelligent Service Gateway (ISG) reloads when you enter the **show pxf cpu iedge ip-session vcci** *vcci id* command.

  Conditions: This symptom is observed when existing sessions are in the process of being disconnected while you enter the **show pxf cpu iedge ip-session vcci** *vcci id* command.

Workaround: Do not enter the **show pxf cpu iedge ip-session vcci** *vcci id* command for sessions that are in the process of being disconnected when the console has a short terminal length.

- CSCsg64438

  Symptoms: When a prepaid service is unapplied from rules, the accounting stop record does not contain packet counts and octet counts.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) when the **service-policy type service unapply name** *policy-map-name* command (in which the *policy-map-name* argument indicates the prepaid service) is configured in the rules.

  Workaround for the packet counts: There is no workaround.

  Workaround for the octet counts: Look for the information in the following attributes that are present in the according stop record:

  ssg-control-info [253] 6 “I<high>;<low>”
  <low> indicates the input octets.

  ssg-control-info [253] 6 “O<high>;<low>”
  <low> indicates the output octets.

- 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.

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

- CSCsg70932

  Symptoms: A Cisco 7200 series that is configured for QoS may crash when traffic is sent.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 or NPE-G2 and that has a Port Adapter Jacket Card in which a 2-port OC-3/STM-1 POS port adapter (PA-POS-2OC3) in installed that has an interface with a service policy.

  Workaround: There is no workaround.

- CSCsg71993

  Symptoms: A DHCP client fails to receive an IP address from the DHCP server.

  Conditions: This is observed on a Cisco router that functions as an Intelligent Service Gateways (ISG) and DHCP server when the **initiator dhcp** IP subscriber configuration command is not enabled.

  Workaround: Enter the **initiator dhcp** IP subscriber configuration command, either with or without the optional **class-aware** keyword.

- CSCsg72388

  Symptoms: A router crashes when a policy that uses a class map of the following form is configured in a policy map and applied to an interface:

  ```
  class-map match-any <classname>
      match <any match criteria>
      match ip rtp <odd number> 0
      <zero or more match clauses>
  ```

  Before the router crashes and enters the ROMmon prompt, the following error message is generated:

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

Conditions: This symptom is observed when you try to match on a range of zero UDP ports with a starting port number that is an odd number. Because the **match ip rtp** command can match only even-numbered ports, this configuration is equivalent to saying “match nothing.”

Workaround: Specify an even-numbered starting port or a non-zero port range.

- 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.

- CSCsg85441

  Conditions: When you configure a large number of individual PVCs (about 52,000) and enter the **show running-config** command, it may take about 50 seconds before the command output is displayed.

  Symptoms: This symptom is observed on a Cisco 10000 series that has a PRE-3 but may also affect other platforms.

  Workaround: There is no workaround.

- CSCsg93274

  Symptoms: When a switchover occurs on the standby PRE, the router does not sent a ciscoRFSwactNotif notification.

  Conditions: This symptom is observed on a Cisco 10000 series when the CISCO-RF-MIB traps are enabled for host that are configured to receive traps, that is, for valid SNMP hosts that have the **snmp-server enable traps rf** command enabled.

  Workaround: Configure SNMPv2 “informs.”

  Alternate Workaround: Use a static ARP configuration for the trap handlers that are configured via the **snmp-server host** command to increase the chances that the first few traps that are sent by the Cisco 10000 series are received by these trap handlers.

TCP/IP Host-Mode Services

- CSCef52888

  Symptoms: Path MTU Discovery (PMTUD) may incorrectly select a higher MTU for an egress interface and may cause BGP to send packets that are larger than the size that the egress interface can support. When this situation occurs, packets are lost and the BGP session may be terminated.

  Conditions: This symptom is observed when PMTUD is enabled over parallel links with different MTUs and when the paths in each direction use different links. Some other conditions may also apply, such as CEF and load-balancing being enabled.

  Workaround: Enter the **ip tcp mss** command to configure the MSS to be less than the MTUs of all possible egress interfaces, or configure the MTUs of all possible egress interfaces to be same as the MSS.

- CSCse28222

  Symptoms: A router that is configured for NSR crashes and generates TCP tracebacks.

  Conditions: This symptom is observed on a Cisco router when a switchover occurs.

  Workaround: There is no workaround.

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.

- CSCek47644

  Symptoms: PPP keepalives are processed at in the slow path.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a broadband remote access server (BRAS) in an HA configuration and that has a virtual-template interface. The symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCek48265

  Symptoms: When you enter the **default ppp bcp tagged-frame** command, a traceback message may be generated on the console.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB and that is configured for PPP.

  Workaround: There is no workaround.

- CSCek55136

  Symptoms: A Cisco 10008 router may restart because of a bus error.

  Conditions: This symptom is observed on a Cisco 10008 router that runs Cisco IOS Release 12.3(7)XI7b and that is configured for PPPoE. However, the symptom appears to be platform-independent and may also affect other releases.

  Workaround: There is no workaround.

- CSCek55209

  Symptoms: When the **ppp multilink endpoint mac** *lan-interface* command or the **ppp multilink endpoint ip** *ip-address* command is configured, the router may unexpectedly reload if the multilink interface goes to the DOWN state, for example, when a PVC virtual circuit is unconfigured.

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

  Workaround: There is no workaround. Do not use these configuration commands in Cisco IOS Releases 12.3, 12.4 or 12.2SB without a fix for this DDTS.

- CSCek56250

  Symptoms: A router may reload while executing the **show ppp multilink** command.

  Conditions: This symptom is observed when a multilink bundle goes down while the output is being generated.

  Workaround: There is no workaround.

- CSCsc30497

  Symptoms: When NAS-port based pre-authorization fails, the PPPoE session limit per VLAN is no longer applied, that is, the local limit is no longer applied to a particular interface.

Conditions: This symptom is observed in Cisco IOS Release 12.3YM but may also occur in other releases.

Workaround: There is no workaround.

- CSCsd45915

  Symptoms: After a switchover has occurred, a virtual-access interface is created instead of a full virtual-access subinterface.

  Conditions: This symptom is observed on a Cisco router that is configured for PPP when a full virtual-template interface is first deleted and then reconfigured.

  Workaround: There is no workaround.

- CSCsd75854

  Symptoms: A router may generate a malformed PPPoE Active Discovery Offer (PADO) packet with two 802.1q tags. The first 802.1q tag contains the correct VLAN ID.

  Conditions: This symptom is observed on a Cisco router when the Service-Name field in the PPPoE Active Discovery Initiation (PADI) packet is empty and not equal to the one that is configured on the router.

  Workaround: Ensure that a correct Service-Name field in used in the PADI packet.

- CSCse05777

  Symptoms: A router may reload unexpectedly when you configure more multilink interfaces than the maximum number that the router can support. The router should not reload but should generate an error message.

  Conditions: This symptom is observed on any Cisco router that imposes a limit on the number of multilink interfaces.

  Workaround: Do not exceed the maximum number of multilink interfaces.

- CSCse29596

  Symptoms: PPPoA sessions cannot be brought up again after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco router when PPPoA sessions are first brought up on the active RP, then brought down by the peer, and then an SSO switchover occurs.

  Workaround: There is no workaround.

- CSCse66625

  Symptoms: A router does not accept the **pppoe max-sessions** *number* command on a subinterface.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB.

  Workaround: First configure the **pppoe max-sessions** *number* command on a BBA group, then attach this BBA group to the subinterface.

- CSCse78652

  Symptoms: The queuing mode on multilink interfaces erroneously defaults to fair-queuing instead of FIFO, causing distributed Cisco Express Forwarding (dCEF) to fail.

  Conditions: This symptom is observed on a Cisco 7500 series and occurs for all multilink interfaces. However, the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCse78979

  Symptoms: PPPoA sessions do not synchronize to the standby PRE while VCs are recreated with a changed encapsulation type.

Conditions: This symptom is observed on a Cisco 10000 series when you change the encapsulation type on the interface from MUX to SNAP and then back to MUX while PPPoA sessions are coming up. The symptom may be platform-independent.

Workaround: There is no workaround.

- 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.

- CSCsf12042

  Symptoms: PPP over Ethernet over Ethernet (PPPoEoE) and PPPoE over Q-in-Q (PPPoEoQ-in-Q) sessions fail to be established.

  Conditions: This symptom is observed on a Cisco router when the connections are made via Fast Ethernet or Gigabit Ethernet interfaces. Note that the symptom does not affect PPP over Ethernet over ATM (PPPoEoA) sessions.

  Workaround: There is no workaround.

- CSCsg31095

  Symptoms: Per-user DNS and WINS attributes are ignored.

  Conditions: This symptom is observed on a Cisco router when RADIUS returns per-user DNS and WINS attributes that are the last attributes for the user profile.

  Workaround: Move the DNS and WINS attributes to a position in the RADIUS profile that ensures that they are not the last attributes.

- CSCsg34400

  Symptoms: A Cisco router that functions as a LAC may crash.

  Conditions: This symptom is observed when a PPPoE session is cleared by the client.

  Workaround: There is no workaround.

- CSCsg38412

  Symptoms: When a Multilink PPP (MLP) session is established over an ISDN link, IPCP fails to negotiate. When the **debug ppp negotiation** command is enabled, you can see that IPCP packets from the peer are not processed. The output of the **show interface** command for the ISDN D-channel interface shows that the input queue limit is 0.

  Conditions: This symptom is observed when the ISDN BRI or PRI interface is not configured as part of a dialer rotary group or dialer pool and when RADIUS is used to assign the multilink bundle to a VRF.

  Workaround: Enter the **dialer rotary-group** command to assign the ISDN interface to a dialer.

Resolved Caveats—Cisco IOS Release 12.2(28)SB13

Cisco IOS Release 12.2(28)SB13 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB13 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCec00268

  Symptoms: A multilink interface may stop processing received packets.

  Conditions: This symptom is observed on a Cisco 7500 series when Multilink PPP (MLP) is configured and when a lot of traffic is forwarded to the process-switching path.

  Workaround: To clear the symptom, move the physical interfaces to a new multilink interface with a new interface number.

- CSCej45747

  Symptoms: On an interface or bundle that is configured with a policy map that is defined with the **bandwidth** *percentage* or **priority** *percentage* command, when the bandwidth on the interface or bundle changes, the bandwidth percentages appear as fixed bandwidths in the output of the **show** *interface* command.

  When the bandwidth on the interface or bundle decreases, the policy map is unexpectedly removed or suspended, and an error message such as the following is generated:

  ```
  BWFQ: Not enough available bandwidth for all classes Available 4096 (kbps) Needed 5777
  (kbps)
  ```

  This situation occurs even though there is sufficient bandwidth to satisfy the fixed and percentage bandwidth requirements.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(25)S.

  Temporary Workaround: Re-attach the policy. However, the symptom may occur again.

- CSCek71844

  Symptoms: When the **virtual-profile** command is configured, PPP sessions do not come up.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCsa53394

  Symptoms: When SNMP traps are generated on a Cisco IOS router, the **show alignment** command displays spurious memory access and tracebacks in the Open Shortest Path First (OSPF) trap generation routine.

  Conditions: The symptoms occur on a router running Cisco IOS Release 12.2(18) SX with the OSPF MIB.

  Workaround: There is no workaround.

- CSCsa73179

  Symptoms: Memory corruption, possibly leading to a crash or other undesired behavior, can occur when the **no default-information originate** command is entered in router RIP configuration mode.

  Conditions: This symptom occurs only if both the RIP routing protocol and the OSPF routing protocol are configured on a router.

Workaround: There is no workaround.

- CSCsd26832

  Symptoms: Traceback errors may be found while using the **no shape average** command under a standalone policy-map.

  Conditions: The symptoms are observed when creating a flat policy-map with shape average and then removing the shape.

  Workaround: There is no workaround.

- CSCsd36670

  Symptoms: CDP may not be enabled with snmpset.

  Conditions: The symptom is observed when CDP is globally disabled and when the user attempts to enable CDP from SNMP.

  Workaround: Enable CDP from CLI.

- 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 T1s.

  Workaround: A router reload clears the issue.

- CSCsg35077

  Symptoms: A device that is running Cisco IOS software 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 Cisco IOS software 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 **no crypto isakmp enable** command 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 Problem Description: This bug is triggered deep into the IKE negotiation, and an exchange of messages between IKE peers is necessary.

  If IPsec is not configured, it is not possible to reach the point in the IKE negotiation where the bug exists.

- 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.

- CSCsi15304

  Symptoms: A router may crash when you remove a PBR configuration from a virtual access interface.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Do not configure PBR on an interface that is used for user sessions.

- CSCsi26038

  Symptoms: After the removal and re-insertion of a PCMCIA flash card from a Cisco 10000 series PRE2, the PRE2 may crash.

  Conditions: The symptoms are observed when a PCMCIA flash card is removed from, and re-inserted into, a Cisco 10000 series PRE2.

  Workaround: There is no workaround.

- CSCsi46184

  Symptoms: Cisco IOS crash is observed when removing PCMCIA flash card.

  Conditions: This crash can occur when the flash card is removed during a read to the card.

  Workaround: Do not remove flash card when it is in use.

- CSCsi61723

  Symptoms: A router may crash spontaneously and display the following message:

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

  Conditions: The symptom is observed on a router that is running Cisco IOS Release 12.2SB. RIP packets that go through many features in this environment (such as, RIP -> IP -> MLP -> PPP -> L2TP -> IP -> QoS/HQF -> driver) may also cause the stack overflow.

  Workaround: There is no workaround.

- CSCsj88665

  Symptoms: A device with a PA-MC-2T3+ may reset because of a bus error if a channel group is removed while the **show interface** command is being used from another telnet session at the same time, and then the telnet session is cleared.

  The device may also display Spurious Memory Accesses.

  Conditions: These symptoms have been observed in the latest Cisco IOS 12.4T and 12.2S releases.

  Workaround: Do not remove a channel group while using the **show interface** command for that interface.

- CSCsk64158

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCsl54880

  Symptoms:

  – Gigabit Ethernet SPA will accept the multicast frames even though it is not destined for it.

  – Enabling bridging on Cisco 7304 SPA will break IP routing.

  Conditions:

  – Send multicast traffic which is not destined to that SPA.

  – Enable bridging and routing on the same interface.

  Workaround:

  1. Enable routing and bridging on separate interfaces.

  2. Enable both routing and bridging on the onboard Gigabit interface.

  Further Problem Description: Both the above mentioned problems are happening because of the TCAM table entry.

- CSCsl61127

  Symptoms: An NSE-150 reloads unexpectedly when the **show pxf crash** command is entered.

  Conditions: Router is running Cisco IOS Release 12.2(31)SB3 or a later rebuild.

  Workaround: Do not use the **show pxf crash** command. Cisco IOS Releases 12.2 (31)SB2 and earlier releases are not affected.

- CSCsl62626

  Symptoms: A Cisco 7304 router may experience high CPU utilization (90-99%) when a large number (such as 2000) FR-L2TPv3 circuits are configured on a POS interface facing the CE router.

  Conditions: A Cisco 7304 router that is configured with an NSE-100 and that is running Cisco IOS Release 12.2(33)SB.

  Workaround: No other workaround than to reduce the scale of the circuits configured.

  Further Problem Description: CPU utilization is proportional to number of FR- L2TPv3 circuits. So the issue occurs for any number of FR-L2TPv3 circuits, but rises gradually as the number of circuits increase.

- 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.

- CSCsm23764

  Symptoms: A device keeps reloading every 50 minutes.

  Conditions: The issue will occur only if the standby RP gets reloaded while CEF is part-way through synching initial data to the standby RP before standby hot state is reached in SSO mode.

  Trigger: Removal or reload of standby before CEF initial synch is complete.

  Impact: This issue affects operations.

Workaround: Reload the active PRE if this issue occurs.

- 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

- CSCsm27979

  Symptoms: A router crashes with "Address Error (load or instruction fetch) exception" when the **show ip vrf** *vrf-name* command is used.

  Conditions: On one vty session, enter the **show ip route vrf** *vrf-name* command and leave it in the "more" condition. From other user interface session, go to configuration mode, and then enter the **no ip vrf** *vrf-name* command using the same VRF name. After at least 5 minutes, the router will crash after hitting the any key on the session that is doing the **show ip vrf** command.

  Workaround: Make sure that there is no **show ip route vrf** command pending before entering the **no ip vrf** command.

- CSCsm47944

  Symptoms: A Gigabit interface on an NSE150 flaps.

  Conditions: This symptom is observed under a high traffic load.

  Workaround: There is no workaround.

  Further Problem Description: This problem is usually caused by defective hardware (SFP, cable, NSE board). Those were swapped, and the problem persisted.

- CSCsm62038

  Symptoms: A Cisco 7300 with an NSE-100 crashes.

  Conditions: This symptom is observed if you configure a hierarchical policy map with a SET command in the second level. The "set" command is *not* supported in the second level policy in the PXF.

  Workaround: Do not configure SET in the second level of a hierarchical policy map.

  Further Problem Description: Because it is not a supported configuration, the router will not accept that configuration in the future.

- CSCsm65976

  Symptoms: An MLP PPP session is not installed into the correct VRF.

  Conditions: This symptom is observed when the VRF is configured as peruser or service profile through the "ip:vrf-id ..." "ip:unnumbered ..." VSAs.

  Workaround: Use the following:

  lcp:interface-config=ip vrf forwarding <vrf> lcp:interface-config=ip unnumbered <loopback interface>

- CSCsm83777

  Symptoms: An address error crash occurs while running Cisco IOS Release 12.2 (31)SB11. Decodes indicate a Layer 4 redirect.

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

  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** is 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.

- CSCso04657

  Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

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

- CSCso09458

  Symptoms: SPAs in an MSC-100 may go missing.

  Conditions: The symptom is observed when you have entered the **hw- module slot slot_num stop** command, then do a switchover and then enter the **hw-module slot slot_num start** command in a new active.

  Workaround: Enter the command **hw-module subslot slot_num reload**.

- CSCso18630

  Symptoms: SNMP counters on the 64-bit counters for incoming traffic, ifHCInOctets, are reporting very high values, different from what CLI reports, and even greater than the physical interfaces capacity.

  Conditions: This symptom may be seen with all line cards (PA-CC, SPA, LCs) on a Cisco 7300 router with NSE-100 that is running c7300-p-mz.122-31.SB10.bin.

  Workaround: There is no workaround.

- CSCso47048

  Symptoms: A router may crash with the following error message:

  ```
  %SYS-2-CHUNKBADFREEMAGIC: Bad free magic number in chunk header, chunk 6DF6E48 data
  6DF7B48 chunk_freemagic EF430000 -Process= "Check heaps", ipl= 0, pid= 5,

  -Traceback= 0x140C170 0x1E878 0x1EA24 0x1B4AC 0x717DB8 chunk_diagnose, code = 2 chunk
  name is PPTP: pptp_swi

  current chunk header = 0x06DF7B38 data check, ptr = 0x06DF7B48

  next chunk header = 0x06DF7B70 data check, ptr = 0x06DF7B80

  previous chunk header = 0x06DF7B00 data check, ptr = 0x06DF7B10
  ```

  Conditions: Issue has been seen on Cisco 7200 router with NPE-G2 configured for L2TP and running Cisco IOS Release 12.4(15)T3 and Cisco IOS Release 12.4(15)T4.

Workaround: There is no workaround.

- CSCso76044

  Symptoms: Whenever a subinterface is created on ESR-6OC3/P-SMI with Cisco IOS c10k2-k91p11-mz.122-31.SB9a, it sends an error. It works fine with Cisco IOS Release 12.2(27)SBB4c.

  Conditions: Unknown.

  Workaround: There is no workaround.

- CSCsq30252

  Symptoms: An E1 controller may flap due to RMAI alarms, even after an internal loop in ESR (with internal clocking) is added.

  Conditions: The symptom is observed on an ESR that is running Cisco IOS Release 12.2(31)SB.

  Workaround: Use the **temux force workaround ds1e1 x y** command.

  Further Problem Description: This issue appears to be corner case.

- CSCsq49176

  Symptoms: Router bus error crash on invalid address:

  ```
  System returned to ROM by bus error at PC 0x608BB8A4, address
  0xC6000E8E
  Address Error (load or instruction fetch) exception, CPU signal 10, PC =
  0x608BB8A4
  -Traceback= 608BB8A4 608EE2F4 600132B8 605B2140 60A26C20 605B1C54 605B2FB4
  ```

  Conditions: Occurred on a Cisco 7200 running Cisco IOS Release 12.2(28)SB6.

  Workaround: There is no workaround.

- CSCsr13399

  Symptoms: Topology:

  Router PPPoE/PPPoA <----> 7301.

  The PPP session is established with the Cisco 7301, which is ISG enabled.

  When traffic reaches 1 gigabyte, the accounting attribute will be corrupted with 2^32 - 1.

  The expectation of the gigabyte word is when it reaches 4294967295 bytes, it will increment with one gigaword.

  The problem is seen in the following releases:

  Cisco IOS Release 12.2(31)SB11: per-user service account corrupts the gigaword, and per-user session is correct.

  Cisco IOS Release 12.2(31)SB12: per-user service account corrupts the gigaword, and per-user session does not show anything at all.

  Cisco IOS Release 12.2(33.1.10)SB1: per-user service account shows nothing in the gigaword, and per-user session is correct.

  Conditions: When traffic reaches 1 gigabyte, the accounting attribute will be corrupted with 2^32 - 1.

  Workaround: There is no workaround.

- 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

- CSCsr90703

  Symptoms: A Cisco 7300 NSE-100/NSE-150 may crash while executing the egress netflow feature in PXF.

  Conditions: The symptom is observed while executing the egress netflow feature in PXF (for example, using the **ip flow egress** or the **mpls egress netflow** commands). More specifically, it occurs when an MPLS packet is sent as an IP packet through an interface with egress netflow configured on it. This results in an invalid VRF index and leads to a PXF crash.

  Workaround: Other than disabling egress netflow on interfaces or disabling PXF altogether (with the **no ip pxf** command), there is no workaround.

- CSCsr93441

  Symptoms: After deleting and configuring back some timeslots for an ESR-4OC3-CHSTM1 card, the PRE3 of a Cisco 10000 series router crashes for a TLB exception. The same issue happens three minutes later when the same steps are applied to the backup PRE.

  Conditions: This symptom is observed after an upgrade to PRE3 and Cisco IOS Release 12.2(33)SB.

  Workaround: There is no workaround.

- 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.

- CSCsv17542

  Symptoms: Traceback may be seen during an ISSU upgrade.

  Conditions: The symptom is observed when doing an ISSU upgrade from Cisco IOS Release 12.2(28)SB12 to Release 12.2(28)SB13.

  Workaround: There is no workaround.

  Further Problem Description: One of the error messages is being printed unconditionally, causing the tracebacks to be seen. The tracebacks are not impacting the ISSU functionality.

- CSCsv57851

  Symptoms: A Cisco 7304 router with an NSE-100 may crash when issuing the **show pxf crash** command.

  Conditions: The symptom is observed on a Cisco 7304 router with an NSE-100 that is running Cisco IOS Release 12.2(28)SB. It is seen when issuing the **show pxf crash** command.

  Workaround: There is no workaround.

  Further Problem Description: The problem is not seen on a Cisco 7304 NSE-150 router.

- CSCsv79786

  Symptoms: A router may crash when hc_poll is polling the counter and the hc_counter_deregister frees it because of an OIR.

  Conditions: This issue is seen with Cisco IOS Release 12.2(28)SB13.

  Workaround: There is no workaround.

  Further Problem Description: This is a corner case and is difficult to hit. The problem is due to the access of an already freed pointer.

Resolved Caveats—Cisco IOS Release 12.2(28)SB12

Cisco IOS Release 12.2(28)SB12 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB12 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCek75633

  Symptoms: A router may crash resulting in service impact.

  Conditions: This symptom is observed on a 7200 router with NPEG2 when you attach a VC class to an ATM bundle. This is platform-independent. On other platforms a crash will not occur only traceback errors are noticed

  Workaround: There is no workaround.

- CSCsl46665

  Symptoms: Interface flap may be noticed during ISSU/MDR on interfaces associated with OC3POS cards.

  Conditions: This issue is observed on performing ISSU/MDR from old label.

  Workaround: There is no workaround.

- CSCsl98665

  Symptoms: Multilink bundles fail to come up.

  Conditions: This problem will be seen only if the bundle has 10 members associated with it.

  Workaround: Remove one member from the bundle, by removing the **ppp multilink group** command, and then do a **shut/no shut** of the bundle.

  Further Problem Description: If we try to bring up a bundle that has 10 members, the bundle will fail to come up. If the bundle has less than 10 members, we will not see this issue.

- CSCsm68773

  Symptoms: LFI bundles will not come up.

  Conditions: The commit of CSCsl98665 disturbed the single member bundle creation.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(28)SB11

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(28)SB11. All the caveats listed in this section are open in Cisco IOS Release 12.2(28)SB10. This section describes only select caveats.

- CSCsl98665

  Symptoms: Multilink bundles fail to come up.

  Conditions: This problem will be seen only if the bundle has 10 members associated with it. The problem does not occur when a bundle has fewer than 10 members.

  Workaround: Remove one member from the bundle, by removing the **ppp multilink group** command, and then perform a **shut/no-shut** of the bundle.

Resolved Caveats—Cisco IOS Release 12.2(28)SB11

Cisco IOS Release 12.2(28)SB11 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB11 but may be open in previous Cisco IOS releases.

IP Routing Protocols

- 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 aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
  aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
  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/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/part05/schat hor. htm
- ACS 4.1 Command Authorization Sets
  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windo ws/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_windo ws/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/netsol/ns696/networking_solutions_white_paper09186a00801ee 18d.sh tml

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/application/pdf/en/us/guest/products/ps1838/c1244/cdccont_0900aecd8 04 ac831.pdf
- Improving Security on Cisco Routers
  http://www.cisco.com/warp/public/707/21.html

- CSCei93982

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

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

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

Workaround: There is no workaround.

- CSCek74752

  Symptoms: In standby the following commands are not displayed when viewing running configuration: **connect atom_1 POS4/0 500 l2transport xconnect 9.0.0.3 100 encapsulation mpls**

  Conditions: Occurs on a Cisco 7600 router.

  Workaround: There is no workaround.

- CSCek76933

  Symptoms: A router may crash when you configure an ATM PVC on an ATM point-to-point subinterface.

  Conditions: This symptom is observed on a Cisco router when the ATM point-to-point subinterface is already part of a bundle.

  Workaround: Configure the ATM PVC on an ATM multipoint subinterface.

- 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.

- CSCsh15456

  Symptoms: A router may crash when you remove a QoS policy from an interface or modify the policy map.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 when you configure a QoS policy, attach it to the interface, run traffic, and then, after a long time, remove the QoS policy or modify the policy map.

  Workaround: There is no workaround.

- CSCsi11314

  Symptoms: After a forced switchover has occurred, ATM subinterfaces may not forward certain packets.

  Conditions: This symptom is observed on a Cisco 7304 that has redundant NSE-100 route processors and that is configured for Reverse Path Forwarding (RPF). The symptom occurs only for ATM subinterfaces on which PVCs are configured.

  Workaround: Disable RPF.

- CSCsi63223

  Symptoms: Control plane policy does not work on Cisco 7500 router. Policy counters do not increase, and match protocol is not accepted in class-map in Cisco IOS Release12.2(31)SB4 images.

  Conditions: Occurs on Cisco 7500 routers running Cisco IOS Release 12.2(31)SB4 configured as follows:

  1. Configure service policy with polices packets based on class they match to say “match icmp any any” send ICMP traffic to routers match counters will increase but not policy counters.
  2. Specify match protocol as classification criteria in class map.

  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.

- CSCsj21036

  Symptoms: The **vbr-rt** and **cbr** commands are not supported when configuring PA-A3 and PA-A6 cards.

  Conditions: Occurs on a Cisco 7304 router.

  Workaround: There is no workaround.

- CSCsk32296

  Symptoms: NAS crashes when sending invalid account session ID.

  Conditions: None.

  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.

- CSCsk62754

  Symptoms: After PRE3 failover, secondary PRE will continuously reboot.

  Conditions: Occurs when a ESR-HH-1GE is installed and with minimal configuration.

  Workaround: There is no workaround.

- CSCsk65987

  Symptoms: HA sync message handling of InARP map results in buffer overflow copy.

  Conditions: This issue is seen only in HA test scenario and also with large Subif I/F name and large VPI/VCI number.

  Workaround: Use the small number for Subif and VPI/VCI.

- CSCsk88270

  Symptoms: A router crashes on bootup due to column 3 memory exception.

Conditions: This symptom is observed on a Cisco 7304 NSE-100 Revision C (or EARLIER) that is running Cisco IOS Release 12.2(32)SR image built between 10/01/2007 and 10/16/2007.

Workaround: There is no workaround.

- CSCsl37493

  Symptoms: PPP renegotiates on the far end router when it receives a CONFREQ from the head end router during a PRE failover on the head end router. SSO state was verified prior to the PRE failover on the head end router.

  Conditions: This symptom was observed in Cisco IOS Release 12.2(28)SB4c and Release 12.2(28)SB10. It was also seen in first engineering image Cisco IOS Release 12.2(28)ZX.

  Workaround: There is no workaround.

- CSCsl52481

  Symptoms: Multilink interfaces fail to come up for LFIoFR after router bootup.

  Conditions: Multilink bundles fail to come up for LFIoFR configuration.

  Workaround: There is no workaround.

- CSCsm19663

  Symptoms: Router crashes when MPLS VPN configurations are applied.

  Conditions: Occurs with the following configuration:

  ```
  72a(config-if)# interface a1/0.1 point-to-point
  72a(config-subif)# mpls ip
  72a(config-subif)# mpls label protocol ldp
  72a(config-subif)# ip address 10.0.0.2 255.0.0.0
  72a(config-subif)# no ipv6 address
  72a(config-subif)# ip split-horizon
  72a(config-subif)# pvc 6/100
  72a(config-if-atm-vc)# encaps aal5snap
  72a(config-if-atm-vc)# exit
  72a(config-subif)# no shut
  ```

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(28)SB10

Cisco IOS Release 12.2(28)SB10 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB10 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsg39295

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

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

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

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

IP Routing Protocols

- 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.

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
                          00000000011111111112222222222333^
                          12345678901234567890123456789012|
                                                          |
                                                       PROBLEM
                                                      (Variable Overflowed).
```

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

- CSCek77702

  Symptoms: An IP address that is configured for an IMA bundle on a PA-A3-8T1IMA port adapter may become lost after an online insertion and removal (OIR) of the port adapter.

  Conditions: This symptom is observed on a Cisco 7304 when a PVC is configured on the IMA main interface on the PA-A3-8T1IMA port adapter and when there is continuous traffic.

  Workaround: There is no workaround.

- CSCek79184

  Symptoms: The active RP may crash when the standby RP comes up.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for high availability (HA) when the NVRAM and standby NVRAM have a non-zero size in the startup configuration and private configuration. The symptom occurs when either of the following conditions are present:

  - The active RP runs Cisco IOS Release 12.2(28)SB7, Release 12.2(28)SB8, or Release 12.2(28)SB9 and the standby RP boots with Release 12.2(28)SB6 or an earlier release, that is, the software image that runs on the active RP has the fix for caveat CSCsd81275 but the software image that runs on the standby RP does not.
  - The active RP runs Release 12.2(28)SB7, Release 12.2(28)SB8, or Release 12.2(28)SB9 and the standby RP boots with Release 12.2(31)SB, that is, the software image on the active RP has the fix for caveat CSCsd81275 but the software image that runs on the standby RP does not.

Workaround: In a live network, the active RP and standby RP usually run the same software images. However, when you perform an upgrade or downgrade of a software image, follow these steps:

1. Copy the running configurations to some devices other than NVRAM by entering the following commands:

copy running-config disk0:/saved-config

copy running-config stby-disk0:/saved-config

2. Erase the NVRAM and standby NVRAM by entering the following commands:

erase nvram: erase stby-nvram:

3. Boot the standby RP with the software image that you intend to upgrade or downgrade. (Without the fix for caveat CSCsd81275: Release 12.2(28)SB6 or an earlier release, or Release 12.2(31)SB. With the fix for caveat CSCsd81275: Release 12.2(28)SB7, Release 12.2(28)SB8, or Release 12.2(28)SB9.)
4. When the standby RP comes up, initiate an RP switchover to enable the new standby RP to boot with the upgraded or downgraded software image by entering the following command:

redundancy force-switchover

Note that no filesystem operations should have been performed during Step 3 and Step 4.

5. Restore the configurations by entering the following commands:

copy disk0:/saved-config running-config

write memory

Further Problem Description: The fix for this caveat prevents the symptom from occurring when either one of the conditions that are mentioned in the Conditions section occur.

However, the crash still occurs when the active RP runs Release 12.2(28)SB7, Release 12.2(28)SB8, or Release 12.2(28)SB9, all of which have the fix for caveat CSCsd81275 but do not have the fix for CSCek79184, and when the standby RP boots with Release 12.2(28)SB10 that has the fix for both caveat CSCsd81275 and CSCek79184. For this situation, there is no workaround.

- CSCek79367

  Symptoms: The **xconnect** *ip address vcid* **pw-class** *class-name* command may not be nvgened when it is entered along with the **backup peer** *ip address vcid* **pw-class** *class-name* command, and the parser submode “cfg-if-atm-l2trans-pvc-xconn” may not be entered.

  Conditions: This symptom is observed on a Cisco 7304 that has an ATM interface when the encapsulation on the L2transport VC is ATM adaptation layer 0 (AAL0).

  Workaround: There is no workaround.

- CSCsa61523

  Symptoms: The following error message is generated on a Cisco 7200 series that has Multilink PPP (MLP) configured on serial interfaces of a PA-MC-STM-1 port adapter:

```
%SYS-2-BADSHARE: Bad refcount in datagram_done, ptr=3, count=0
```

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.3(11)T3 only when MLP is configured on the serial interfaces. The symptom may also occur in other releases.

  Workaround: Unconfigure MLP on the serial interfaces.

- CSCsd75273

  Cisco Catalyst 6000, 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 on t hem are affected. This vulnerability affects systems that run Internetwork Operating System (IOS) or Catalyst Operating System (CatOS).

  Cisco has made free software available to address this vulnerability for affected customers.

  A Cisco Security Advisory for this vulnerability is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070228-nam.shtml

- CSCse52951

  Cisco Catalyst 6000, 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 on t hem are affected. This vulnerability affects systems that run Internetwork Operating System (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

- CSCse79790

  Symptoms: When PPPoE Relay is configured, only one session comes up successfully. All successive sessions fail. The initiation of more sessions brings down the existing sessions. If there are active sessions that are already existing (not necessarily PPPoE Relay sessions), the initiation of new PPPoE Relay sessions tears down all the sessions.

  Conditions: These symptoms are observed on a Cisco router that functions in a Virtual Private Dialup Network (VPDN). The symptom occurs only for PPPoE Relay sessions and not for normal sessions.

  Workaround: There is no workaround.

- 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.

- CSCsi16819

  Symptoms: An end-to-end ping between CE routers may fail in an ATMoMPLS environment.

  Conditions: This symptom is observed when a Cisco router that functions as a PE router has ATMoMPLS configured as “ATM single cell relay over MPLS: port mode” via the **xconnect** command under an ATM Main interface.

  Workaround: There is no workaround.

- CSCsj05519

  Symptoms: SSO Standby NSE-100 crashes with the following error messages:

  ```
  IDBINDEX_SYNC-3-IDBINDEX_ENTRY_LOOKUP or
  HA_CONFIG_SYNC-3-LBL_POLICY
  ```

  After the crash, it was observed redundancy mode changed to RPR. When manual reset is applied on the standby, redundancy mode is back to SSO.

  Conditions: This symptom is observed on a Cisco 7300 router that is configured with SSO 2xNSE-100 that is running Cisco IOS Release 12.2(25)S10. The issue seems intermittent and can sometimes be triggered by applying a large configuration (approximately 600 vrfs and 1500 subinterfaces).

  Workaround: There is no workaround.

- CSCsj12883

  Symptoms: Frame Relay service policy counters may not be updated.

  Conditions: This symptom is observed on a Cisco 7304 when that has a POS interface that is configured for Frame Relay with a single DLCI that uses an output service policy. The symptom occurs after the following sequence of events:

  1. You create a point-to-point subinterface that is configured for Frame Relay encapsulation, as in the following example:

  ```
  Current configuration: 143 bytes
  !
  interface POS5/0
   no ip address
   encapsulation frame-relay
   load-interval 30
   clock source internal
   frame-relay intf-type dce
  end

  mft-73b#sh run int pos5/0.1
  Building configuration...

  Current configuration : 182 bytes
  !
  interface POS5/0.1 point-to-point
   ip address 2.2.2.1 255.0.0.0
   snmp trap link-status
   frame-relay interface-dlci 1007
   service-policy input in
  ```

```
 service-policy output out
```

2. You verify the connectivity and service policy outputs by generating traffic. All the QoS counters are updated properly for the service policy on the main interface and subinterface.
3. You remove the point-to-point subinterface, as in the following example:

```
mft-73b#Config t
mft-73b(confgi)# No int  POS5/0.1 point-to-point
```

4. You add the subinterface configuration to the main interface, as in the following example:

```
interface POS5/0
 ip address 2.2.2.1 255.0.0.0
 encapsulation frame-relay
 load-interval 30
 clock source internal
 frame-relay interface-dlci 1007
 frame-relay intf-type dce
 service-policy input in
 service-policy output out
```

5. You generate traffic.
6. You enter the **show policy-map interface** command.

In this situation, the output of the command shows zero for the Frame Relay service policy counters.

Workaround: There is no workaround.

- CSCsj57574

  Symptoms: A success event message is sent for a malformed XML. In this situation, a failure message should be sent.

  Conditions: This symptom is observed when you send a malformed XML via the **cns-send** command, as in the example below:

```
<?xml version="1.0" encoding="UTF-8" ?>^M^M
<config-event config-action="write" no-syntax-check="TRUE">^M^M
<identifier>IDENTIFIER</identifier>^M^M
<config-data>^M^M
   <config-id>AAA</config-id>^M^M
   <cli>access-list 1 permit any^M^M
   <cli>access-list 2 permit any ^M^M
   <cli>access-list 1 permit any ^M^M
   <cli>access-list 2 permit any ^M^M
   <cli>access-list 1 permit any ^M^M
   <cli>access-list 2 permit any ^M^M
   <cli>access-list 1 permit any ^M^M
   <cli>access-list 2 permit any ^M^M
   <cli>access-list 2 permit any ^M^M
   <cli>access-list 2 permit any ^M^M
   </cli>^M^M
   </cli>^M^M
   </cli>^M^M
   </cli>^M^M
   </cli>^M^M
   </cli>^M^M
   </cli>^M^M
   </cli>^M^M
   </cli>^M^M
   </cli>^M^M
</config-data>^M^M
</config-event>^M^M
```

Workaround: There is no workaround.

- CSCsj80375

  Symptoms: A T3/E3 serial SPA may not come up because the line protocol remains down, and the output of the **show controllers serial** command does not generate any output for the T3/E3 serial SPA.

  Conditions: This symptom is observed on a Cisco 7304 when you apply the configuration for the first time after the router has booted.

  Workaround: Unconfigure and reconfigure the **card type** command for the T3/E3 serial SPA.

- CSCsj94561

  Symptoms: A router may crash because of a bus error when you perform an OIR of a PA-MC-8TE1+ port adapter or when you enter the **hw-module slot** *slot-number* **stop** command for the slot in which the PA-MC-8TE1+ port adapter is installed.

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

  Workaround: There is no workaround.

- CSCsk18924

  Symptoms: An NSE-100 crashes after you have applied service policies to approximately 600 VLAN subinterfaces.

  Conditions: This symptom is observed on a Cisco 7304 that has a very large configuration that causes memory exhaustion, for example, 4000 VLAN subinterfaces with nested policy maps that are applied to many of these subinterfaces.

  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

Resolved Caveats—Cisco IOS Release 12.2(28)SB9

Cisco IOS Release 12.2(28)SB9 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB9 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsg19546

  Symptoms: The standby RP may reload unexpectedly because of a Redundancy Facility (RF) synchronization error.

  Conditions: This symptom is observed on a Cisco router that is configured for SNMP, dMLP, and SSO.

  Workaround: Do not configure SSO. Rather, configure RPR+.

IP Routing Protocols

- CSCin95836

  The Cisco Next Hop Resolution Protocol (NHRP) feature in Cisco IOS contains a vulnerability that can result in a restart of the device or possible remote code execution.

  NHRP is a primary component of the Dynamic Multipoint Virtual Private Network (DMVPN) feature.

  NHRP can operate in three ways: at the link layer (Layer 2), over Generic Routing Encapsulation (GRE) and multipoint GRE (mGRE) tunnels and directly on IP (IP protocol number 54). This vulnerability affects all three methods of operation.

  NHRP is not enabled by default for Cisco IOS.

  This vulnerability is addressed by Cisco bug IDs CSCin95836 for non-12.2 mainline releases and CSCsi23231 for 12.2 mainline releases.

  This advisory is posted at

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

- 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.

Miscellaneous

- CSCek34307

  Symptoms: After a service policy is removed from the virtual template, the same policy is not automatically removed from the virtual-access interface.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB or Release 12.2(27)SBC.

Workaround: Clear the virtual-access interface.

- CSCek53559

  Symptoms: A router may reload after receiving a malformed UDP packet on port 67.

  Conditions: This symptom is observed on a Cisco router that functions as an DHCP server.

  Workaround: There is no workaround.

- CSCek66151

  Symptoms: Shaping may not occur on individual VBR-nrt VCs, and there may be no throughput on UBR VCs.

  Conditions: These symptoms are observed on a Cisco router that has a line card that is configured for T3 with the PLCP frame format and the M23 ATM framing method.

  Workaround: There is no workaround.

- CSCek71346

  Symptoms: The MPLS forwarding table is not shown on a router, causing packet drops in end-to-end connectivity across the MPLS cloud.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router after a switchover has occurred.

  Workaround: There is no workaround.

- CSCek73621

  Symptoms: A PA-CC in which a PA-A6 port adapter is installed may crash continuously, preventing the PA-A6 from coming up.

  Conditions: This symptom is observed on a Cisco 7304 after you have entered the **no shutdown** command on an interface of the PA-A6 port adapter.

  Workaround: There is no workaround.

- CSCse17665

  Symptoms: A software-forced reload may occur on a Cisco 7304 that has an NSE-100 or a NSE-150 when you perform an OIR of an MSC-100.

  Conditions: This symptom is observed while the MSC-100 processes a large amount of traffic.

  Possible Workaround: Stop the traffic through the MSC-100 before you perform the OIR by entering the **shutdown** interface configuration command on all the interfaces of the MSC-100. After the OIR, enter the **no shutdown** interface configuration command on all the interfaces of the MSC-100.

- CSCse65884

  Symptoms: The **atm pvp** *vpi* **l2transport** command may disappear from the configuration.

  Conditions: This symptom is observed after you have reloaded the router.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, reconfigure the command.

- CSCsg56947

  Symptoms: When you perform and OIR of a SPA-2XOC3-POS, the HC counters may stop functioning.

Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S10 or a later release or Release 12.2(28)SB5.

Workaround: Do not perform an OIR. Rather, reload the SPA when there is an opportunity.

- CSCsg77139

  Symptoms: After you have reloaded a router, VRF routes disappear.

  Conditions: This symptom is observed when you reload a router the processes a heavy traffic flow.

  Workaround: Enter the **clear ip route vrf** *vrf-name* command.

  Alternate Workaround: Enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the interface from which the VRF routes have disappeared.

- CSCsg98611

  Symptoms: When you enter the **issu loadversion** command, the ISSU may fail with the following error message:

  ```
  Active [ ] and Standby [ ] images should be the same for running loadversion
  ```

  Conditions: This symptom is observed in a rare situation on a Cisco router and occurs even when the Cisco IOS software images on the active and standby RPs are identical.

  Workaround: There is no workaround.

- CSCsg99958

  Symptoms: Queue and buffer leaks may occur, and the output of the **show pxf cpu queue summary** command may show that many queues are being recycled.

  Conditions: This symptom is observed on a Cisco 10000 series that has a class queue configured for a UDP port and occurs after a large number of serial interfaces flap on the router at the far-end.

  Workaround: Add a queue-limit for the class queue on the UDP port, as in the following example:

  ```
  policy-map IPBH
    class udp_traffic
      police percent 90 17 ms 17 ms conform-action transmit exceed-action drop
  violate-action drop
   priority
  queue-limit 512
    class tcp_traffic
      bandwidth percent 9
      queue-limit 256
  ```

- CSCsh05419

  Symptoms: When you paste a large configuration for a channelized port adapter, the standby RP may crash.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for HA.

  Workaround: Copy the configuration for the channelized port adapter to the startup configuration and then reload the router.

  Alternate Workaround: Do not copy the configuration. Rather, enter the configuration manually.

- CSCsh47740

  Symptoms: In an ATM pseudowire configuration, when you reset a line card by entering the **hw-module slot** *slot-number* **reset** command, the pseudowire comes back up but the traffic does not resume, and an end-to-end ping fails.

Conditions: This symptom is observed on a Cisco 10000 series.

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

- CSCsh61595

  Symptoms: Some serial interfaces continuously flap and do not remain in the up state because a PPP negotiation loop occurs.

  Conditions: This symptom is observed on a Cisco 10000 series after a large number of interfaces has flapped from more than two hours.

  Workaround: There is no workaround.

- CSCsh69969

  Symptoms: The rate in the output of the **show ip mroute active** command shows twice the number of packets per second.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsi14211

  Symptoms: A CPUHOG condition may occur when an LDP session goes down.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS LDP, that has more than 30 LDP sessions with peers, and that exchanges more than 5000 label bindings for each LDP session. The symptom occurs when the LDP session goes down shortly after it came up.

  Workaround: There is no workaround.

- CSCsi19863

  Symptoms: A Cisco 7304 that has an NSE-100 may crash when you unconfigure a match statement in a class map.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(31)SB when you enter the **no match ip prec** twice for a class map.

  Workaround: There is no workaround.

- CSCsi20225

  Symptoms: Continuous tracebacks may be generated on an LNS.

  Conditions: This symptom is observed when you bring up PPPoX or L2TP sessions over multiple tunnels without traffic being processed over these sessions.

  Workaround: There is no workaround.

- CSCsi26378

  Symptoms: For FE and GE SPAs, the broadcast counter value in the output of the **show interface** *type slot/port* command may be twice the value as the actual number of broadcast packets that are received by the interface.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with a 4-port 10/100 Fast Ethernet SPA or 2-port 10/100/1000 Gigabit Ethernet SPA.

  Workaround: There is no workaround.

  Further Problem Description: This symptom is specific to the SPA on the Cisco 7304.

- CSCsi32575

  Symptoms: The SNMP input and output counters may not be incremented or may show a wrong value.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and a POS interface that is configured for Frame Relay encapsulation.

  Workaround: Do not use SNMP for information about the input and output counters. Rather, enter the **show frame-relay pvc** command.

- CSCsi57207

  Symptoms: A bus error crash is seen on a Cisco router that is running Cisco IOS Release 12.2(31)SB3.

  Conditions: This symptom is seen when PPPoE/PPPoA is configured with PPP idletimeout and PPP keepalive.

  Workaround: There is no workaround.

- CSCsi57924

  Symptoms: AToM Xconnect end-to-end connectivity may be lost when MAC Address Accounting is configured on the Xconnect circuit.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 or an NSE-150.

  Workaround: There is no workaround.

- CSCsi58871

  Symptoms: For a Gigabit Ethernet interface, the ifOutNUcastPkts may decrement rather than increment.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(28)SB but could also occur in Release 12.2S.

  Workaround: There is no workaround.

- CSCsi58960

  Symptoms: Channelized line cards may reload unexpectedly and an MR-APS failover occurs.

  Conditions: These symptoms are observed on a Cisco 10000 series when packets with a source address of 127.xxx are being processed, causing a PXF crash that triggers a PRE switchover.

  Workaround: Configure an access control list (ACL) to block packets with a source address of 127.xxx.

- 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.

- CSCsi73899

  Symptoms: A Cisco 7301 or Cisco 7304 that is configured to use MPLS service policies on some interfaces may crash. The crash may be preceded by following error messages:

  ```
  %SYS-2-CHUNKBOUNDSIB: Error noticed in the sibling of the chunk pak subblock c, Chunk
  index : 25, Chunk real max :25
  ```

  and

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 45FE855C data 45FE862C
  chunkmagic 15A3C78B chunk_freemagic 1000000
  ```

  Conditions: This symptom is observed on a Cisco 7301 and Cisco 7304 that run Cisco IOS Release 12.2(31)SB and is not related to a specific command sequence. However, note that the crash is platform-independent. For example, the crash could also occur on a Cisco 7600 series that runs Cisco IOS Release 12.2(33)SRB.

  Workaround: There is no workaround.

- 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.

- CSCsj29558

  Symptoms: When you configure the CNS Exec Agent, a traceback and spurious memory accesses may be generated.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2S or Release 12.2SB.

Workaround: There is no workaround. However, the functionality of the CNS Exec Agent is not affected.

TCP/IP Host-Mode Services

- CSCee32814

  Symptoms: TCP source ports that are used for connections that originate from a Cisco IOS platform may be chosen in a predictable manner.

  Conditions: This symptom is observed for outbound TCP connections for which a particular source port is not required.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCek77555

  Symptoms: PPP may not start on a serial interface that is physically up. When this situation occurs, inspection of the interface via the **show interface** command shows that the physical layer is up, but that the line protocol is down, and that LCP is closed.

  Conditions: This symptom is observed only on regular serial interfaces that use PPP encapsulation. The symptom does not occur with tunneling mechanisms such as PPP over ATM (PPPoATM) or VPDN sessions. The symptom may occur when the physical layer undergoes multiple state transitions, starting from an up state and ending in an up state, with the entire sequence occurring over a short period of time. In such a situation, event filtering mechanisms in Cisco IOS software may prevent a notification from being sent to PPP when the link returns to an up state, and, in turn, PPP from (re-)starting on the interface. The most likely time for such a situation to occur is when PPP itself resets the interface, which occurs when an existing PPP session is terminated because of a keepalive failure or LCP negotiation failure.

  Workaround: Any sequence that resets the physical layer and that is slow enough that the filtering mechanisms do not once again intrude is sufficient to restart PPP. For example, you can restart PPP on the interface by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command.

- CSCsi51530

  Symptoms: If non-Cisco PPPoA client is dialing into a Cisco router, the call may fail at the PPP authentication phase. When this situation occurs, the following error message is generated:

  Failed to send an authentication request x

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(31)SB5.

  Workaround: There is no workaround.

- CSCsi82832

  Symptoms: FastStart does not function on PPP interfaces. (FastStart is enabled by default for regular serial interfaces.)

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

Further Problem Description: FastStart acts as a partial solution for the condition that is described in caveat CSCek77555, because FastStart enables an inbound packet from a peer to trigger the startup of PPP (that is, FastStart brings PPP out of the inert state that is documented in caveat CSCek77555).

Resolved Caveats—Cisco IOS Release 12.2(28)SB8

Cisco IOS Release 12.2(28)SB8 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB8 but may be open in previous Cisco IOS releases.

Miscellaneous

- 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.

- CSCsh52756

  Symptoms: A router may crash when you delete or detach a 3-level hierarchical policy from an interface.

  Conditions: This symptom is observed on a Cisco 7304.

  Workaround: There is no workaround.

- CSCsi32607

  Symptoms: A 4-port channelized T3 half-height (ESR-HH-4CT3) line card may generate the following error messages, stop forwarding traffic, and reset unexpectedly:

  ```
  slotindex is X.
  IB Link status: XXXXXXXX

  %C10KEVENTMGR-1-IRONBUS_FAULT: Ironbus Event X/X, Restarting Ironbus X/X Ironbus
  retry:40 ib_stat0:0xXXXX ib_stat1:0xXXX

  %PXF_DMA-3-IRONBUS_NOTRUNNING: Data path to slot X/X failed to synchronize (State Not
  Running)
  X/X Ironbus retry:XX ib_stat0:0xXXXX ib_stat1:0xXXX
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(28)SB6.

  Workaround: There is no workaround. You must reset the line card to bring it back into operation.

- CSCsi40062

  Symptoms: A 4-port channelized T3 half-height line card (ESR-HH-4CT3) resets continuously after a “PXF_DMA-3-IRONBUS_NOTRUNNING” error has occurred.

Conditions: This symptom is observed on a Cisco 10000 series.

Workaround: Shut down all ports on the line card, reseat the line card, re-enable all ports on the line card, and then initiate a switchover to the standby PRE.

Resolved Caveats—Cisco IOS Release 12.2(28)SB7

Cisco IOS Release 12.2(28)SB7 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(31)SB7 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCek63810

  Symptoms: A Cisco 10000 series may run out of memory after a number of ATM port flaps have occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with 28,000 PPPoA Point-to-Point Termination and Aggregation (PTA) sessions. Each time that the ATM ports that carry the sessions flap and in this process remain down long enough for the sessions to time-out, more memory is lost.

  Workaround: There is no workaround.

- CSCsh19482

  Symptoms: A Cisco 10000 series may crash and generate a "%C10K-2-RPRTIMEOUT_CRASH:" error message.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for NetFlow.

  Workaround: There is no workaround.

IP Routing Protocols

- CSCsc96746

  Symptoms: PIM may not choose the path with the highest IP address when it should do so.

  Conditions: This symptom is observed on a Cisco router that functions in a topology with equal-cost RPF paths.

  Workaround: There is no workaround.

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.

- CSCeh71337

  Symptoms: Traffic loss may occur for more than 80 seconds after a high availability (HA) switchover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that has line cards that are configured for Automatic Protection Switching (APS).

  Workaround: There is no workaround.

- CSCei46978

  Symptoms: A Cisco 7200 series may generate the following error message, and links flap:

  ```
  %SBETH-3-ERRINT: GigabitEthernet0/1, error interrupt, mac_status = 0x0000000000840000
  ```

  Conditions: These symptoms are observed on a Cisco 7200 series that is configured with an NPE-G1 and that runs Cisco IOS Release 12.3(15). However, the symptom is not release-specific.

  Workaround: There is no workaround. Note that the symptom does not occur in Release 12.3(13).

- CSCej00340

  Symptoms: A Cisco 7304 crashes when you configure an SVC, unconfigure the SVC, configure a VC, and unconfigure the VC.

  Conditions: This symptom is observed on a Cisco 7304 when you perform the following actions:

  1. Configure an SVC, ping another interface, and unconfigure the SVC.
  2. Configure a VC, and ping another interface.
  3. Unconfigure the VC by entering the following commands:

     ```
     no ip routing
     no ip address ip-address mask
     no atm pvc vcd vpi vci
     aal5snap inarp minutes
     ```

  At this point, the router crashes.

  Workaround: Do not unconfigure a VC by using the method that is indicated in the Conditions above.

  Alternate Workaround: When the router has the **atm bandwidth dynamic** command enabled for an IMA group, remove this command to prevent the router from crashing.

- CSCek24008

  Symptoms: Toggling an output service policy on an interface that processes a high rate of egress traffic may cause the PXF engine to crash.

  Conditions: This symptom is observed only on a Cisco 7304 that has an NSE-100.

  Workaround: There is no workaround.

- CSCek56415

  Symptoms: The Hierarchal Queuing Framework (HQF) is not removed after you have removed a service policy.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 and that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCek61519

  Symptoms: When you continuously perform OIRs of a SPA or port adapter that is installed in a Port Adapter Carrier Card, tracebacks are generated, and the router eventually crashes.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for HA.

  Workaround: There is no workaround.

- 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.

- CSCek64188

  Symptoms: An error message indicating memory leak and pending transmission for IPC messages is displayed as follows:

  ```
  %IPC-5-WATERMARK: 25642 messages pending in xmt for the port Primary RFS Server
  Port(10000.C) from source seat 2150000
  %SYS-2-MALLOCFAIL: Memory allocation of 4268 bytes failed from 0x9F32944, alignment 32
  ```

  Conditions: This issue is triggered by CSCeb05456 and is applicable only if your Cisco IOS image has integrated the fix of CSCeb05456.

  Workaround: Periodically, reload the router so that the IPC buffer pool will be reinitialized.

- CSCek65491

  Symptoms: A router that is configured for HA may unexpectedly reload because of a spurious memory access.

  Conditions: This symptom is observed on a Cisco 10000 series when an L2TP tunnel interface flaps, causing a spurious memory access in the chunk memory. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

  Further Problem Description: Note that SSO is not supported on a Cisco 10000 series that runs Cisco IOS Release 12.2(28)SB or one of its rebuilds and that is configured for broadband aggregation.:

  “In Cisco IOS Release 12.2(28)SB, the Cisco 10000 series supports Route Processor Redundancy Plus (RPR+), and Stateful Switchover (SSO). However for broadband aggregation features, the Cisco 10000 series supports RPR+ only.”

  For more information, see the Broadband Aggregation and Leased-Line Overview document:

  http://www.cisco.com/en/US/products/hw/routers/ps133/
  products_configuration_gu ide_chapter09186a00805057de.html

- CSCek67590

  Symptoms: MFR interfaces do not come up when the router boots.

  Conditions: This symptom is observed on a Cisco 10000 series that runs a Cisco IOS software image that includes the fix for CSCsg86572 and that has MFR interfaces configured on either a 1 port channelized OC-12 line card or a 4-port channelized OC-3 line card. A list of the affected releases can be found at http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsg86572. 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.

- CSCek72665

  Symptoms: Tracebacks may be logged in the console log of the standby PRE.

  Conditions: This symptom is observed on a Cisco 10000 series when a T1 channel group is configured on a T3 controller of 6-port channelized T3 line card.

  Workaround: Reset the standby PRE.

- CSCek73843

  Symptoms: A Cisco 7304 may crash when you enter the **no flowcontrol send** command.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 and a carrier card in which a SPA is installed.

  Workaround: There is no workaround.

- CSCsa65826

  Symptoms: The flow control for an on-board RJ45 GE interface of an NPE-G1 may not function properly.

  Conditions: This symptom is observed on a Cisco 7200 series and a Cisco 7301.

  Workaround: There is no workaround.

- CSCsb12598

  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.

- 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.

- CSCsb65901

  Symptoms: A Cisco 7304 may reload unexpectedly while traffic is flowing.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100, that runs Cisco IOS Release 12.2(20)S9, that is configured for MPLS, and that has PXF processing enabled. The symptom occurs in a two-way loadbalancing scenario in which one link is a GRE tunnel interface that uses a static route. The symptom may also occur in Release 12.2SB.

  Workaround: Do not configure a static route that sends traffic to the tunnel destination through the tunnel interface itself.

- CSCsd81275

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

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

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

  Workaround: There is no workaround.

- CSCsd81407

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

  – Session Initiation Protocol (SIP)

  – Media Gateway Control Protocol (MGCP)

  – Signaling protocols H.323, H.254

  – Real-time Transport Protocol (RTP)

  – Facsimile reception

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

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

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

- 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.

- 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.

- 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/products/ps6441/products_configuration_guide_chapter09186a0080716ec2.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

- 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.

- CSCsf17521

  Symptoms: When there is a hierarchical policy with a Class of Service (CoS), traffic shaping that is applied on the parent policy does not function properly for speeds that are slower than 2000 kbps because the throughput is reduced.

  Conditions: This symptom is observed on a Cisco 7304 when there is a priority class configured in a policy that is attached to an interface. The larger the packets, the more the throughput is reduced.

  Workaround: There is no workaround.

- CSCsf20019

  Symptoms: When traffic is being processed at a low speed such as 56 Kbps, intermittently, traffic comes to a complete halt on a Frame Relay subinterface.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2. The symptom occurs when the PXF engine stops dequeueing packets on the Frame Relay subinterface, causing the interface output queue to become wedged.

  Workaround: Remove the service policy from the subinterface and then re-apply the service policy to the subinterface.

  Further Problem Description: Without applying the workaround, about 60 to 70 minutes after the output queue has become wedged, the output queue starts to dequeue itself.

- CSCsg15342

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

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

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

- 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.

- CSCsg66504

  Symptoms: Traffic is lost for 10 to 15 seconds after a PRE switchover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series immediately after the standby PRE enters the hot standby state.

  Workaround: There is no workaround.

- 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.

- CSCsg75968

  Symptoms: When you enter the **clear counters** command, a Cisco 7304 that has an NSE-150 may crash and generate a TLB exception.

  Conditions: This symptom is observed when the Cisco 7304 is configured with 500 VRFs on an PA-A6 port adapter, when 250 VRFs are active, and when you perform a soft OIR for the PA-A6 and then enter the **clear counters** command.

  Workaround: There is no workaround.

- CSCsg86121

  Symptoms: A POS SPA is unexpectedly deactivated when the traffic flow stops.

  Conditions: This symptom is observed on a Cisco 7304 after the SPA has received a Path Loss of Pointer (PLOP) alarm.

  Workaround: Perform a soft OIR of the SPA by entering the **hw-module subslot** *slot/subslot* **start** command.

- CSCsg87729

  Symptoms: A Gigabit Ethernet interface on a Cisco 7304 that has an NPE-G100 does not support flow control. When the traffic profile results in micro burst on a segment, the output of the **show interface** command may shows overrun errors.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 and that runs Cisco IOS Release 12.2S or Release 12.2SB. Note that the symptom does not occur on a Cisco 7304 that has an NSE-100 or NSE-150.

  Workaround: There is no workaround.

  Further Problem Description: The fix for this caveat enables you to configure flowcontrol in interface configuration mode, thereby allowing pause frames to be sent to the peer. Enable flow control by entering the following commands on the Gigabit Ethernet interface:

  ```
  Router#conf t
  Router(config) # interface gig0
  Router(config-if) # flowcontrol send
  Router(config-if) # end
  ```

  Enable flowcontrol only when autonegotiation is also enabled to allow the NPE-G100 to negotiate with its peers as to whether it can recognize the pause frames.

  Note that an additional change is made via caveat CSCsg39245 to increase the default receive ring limit from 64 Kbps to 128 Kbps to help absorb micro bursts.

- CSCsg90929

  Symptoms: When you configure MR-APS between a Cisco 7304 and another router such as a Cisco 7500 series or Cisco 7600 series with PA-MC-STM-1 port adapters, the following tracebacks are logged on the Cisco 7304:

  ```
  -Process= "APS process", ipl= 0, pid= 191
  -Traceback= 406DC2E0 40741174 400C24BC 400C2BF0 400C6D9C 400C79EC 400C8814 400C8894
  400C90B8
  ```

  Conditions: This symptom is observed on a Cisco 7304 when the working or protect PA-MC-STM-1 port adapter in the active state.

  Workaround: There is no workaround.

  Further Problem Description: The symptom occurs with the following Cisco IOS software images:

  On the Cisco 7304:

  - Release 12.2(27)SBC5 (PGP ver.4)
  - Release 12.2(28)SB5 (PGP ver.4)

  On the Cisco 7600 series:

  - Release 12.2(18)SXD5 (PGP ver.3)
  - Release 12.2(33)SRA1 (PGP ver.4)

- CSCsg97717

  Symptoms: The PXF engine of an NSE-150 crashes when you enter the **ip pim bidir-enable** command.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for MVPN with a single VRF when multicast traffic is flowing through this VRF.

  Workaround: There is no workaround.

- 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.

- CSCsh04911

  Symptoms: On a Cisco 7304 that is configured for AToM, a software-forced reload may occur on an NSE-100.

  Conditions: This symptom is observed when egress NetFlow is configured on an AToM attachment circuit.

  Workaround: There is no workaround.

  Further Problem Description: The configuration that is stated in the Conditions is essentially a misconfiguration. NetFlow can collect information only about Layer 3 IP packets. However, the AToM attachment circuit is transmitting Layer 2 frames, so the egress NetFlow is not valid.

- 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.

- 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.

- CSCsh60482

  Symptoms: An SNMP query for the DS1-MIB does not return any results.

  Conditions: This symptom is observed on a Cisco 7301 that is configured with a channelized T3 port.

  Workaround: There is no workaround.

- CSCsh84765

  Symptoms: After a switchover has occurred and while the standby RP enters the HOT standby state, packet loss may occur accompanied by a CPUHOG condition.

  Conditions: This symptom is observed on a Cisco router that is configured for ISSU or SSO. Packet loss may be more pronounced on a router that has the OSPF Support for Fast Hellos feature enabled.

  Workaround: There is no workaround.

- CSCsh91659

  Symptoms: When a SmartJack is configured in a loopback, the PRE in slot B of a Cisco 10000 series may crash continuously because bulk synchronization fails between the PREs.

  Conditions: This symptom is observed when you enter the **t1** *t1-number* **loopback remote line inband maintenance** command.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, remove all occurrences of the **t1** *t1-number* **loopback remote line inband maintenance** command from the running configuration via the console of the active PRE.

- CSCsh91746

  Symptoms: After creating T1 links on a channelized STM-1 interface, you cannot access the associated interfaces in global configuration mode or Exec mode.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Creating a new interface may clear the condition. If it does not, reload the router.

- CSCsh96616

  Symptoms: When the PXF engine crashes and causes a PRE switchover, traffic outage duration is 3 to 4 seconds longer than with prior software versions.

  Conditions: This symptom is observed on a Cisco 10000 series PRE-2 routing and forwarding engine.

Workaround: There is no workaround to the performance degradation. However, it is possible to configure the system such that a PXF fault does not cause a PRE switchover. Doing so may result in lower overall system availability, since in some cases a PXF restart takes longer to complete than does a PRE switchover. By default, the system will switch to the Standby PRE after two PXF restarts in five hours.

Further Problem Description: The symptom does not occur after a normal PRE switchover, that is, traffic loss does not last longer than in prior software releases.

- 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.

- CSCsi24604

  Symptoms: The output of the **show controllers** and **show aps** commands does not show the 4-port channelized OC-3 line card.

  Conditions: This symptom is observed on a Cisco 10000 series that has a 4-port channelized OC-3 line card that functions in a multirouter APS configuration and occurs after the router has been reloaded.

  Workaround: Enter the **hw-module slot** *slot-number* **reset** command for the affected line card.

- CSCsi25342

  Symptoms: Even after you have removed a T1 line, you still can configure a Facilities Data Link (FDL) on the removed T1 line by entering the **service-module t1 fdl** command. This command should not be accepted because the T1 line is not available.

  Conditions: This symptom is observed on a Cisco 10000 series.

  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.

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

- CSCsi33557

  Symptoms: When you insert or remove a port adapter, the router may generate the following error message and tracebacks:

  ```
  %SYS-2-INTSCHED: ‘suspend’ at level 2
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(28)SB and that is configured for In Service Software Upgrade (ISSU).

Workaround: There is no workaround.

- CSCsi46440

  Symptoms: An error message that indicates an invalid memory action and tracebacks may be generated on a Cisco 10000 series.

  Conditions: This symptom is observed on a Cisco 10000 series that has a large configuration when a switchover occurs of the PRE and a 4-port channelized T3 half-height line card.

  Workaround: There is no workaround.

- CSCsi15995

  Symptoms: Multilink interfaces stop transmitting traffic after a PRE failover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that has two OC-12 ports that function as active ports in an APS configuration and that are configured with multiple multilink interfaces.

  Workaround: Enter the **microcode reload pxf** command. Note that entering the **hw-module subslot** *slot/subslot* **reset** command for the affected ports does not resolve the symptom.

TCP/IP Host-Mode Services

- CSCsb51019

  Symptoms: A TCP session does not time out but is stuck in the FINWAIT1 state and the following error message is generated:

  ```
  %TCP-6-BADAUTH: No MD5 digest from x.x.x.x to y.y.y.y(179) (RST)
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for BGP and that is connected to a third-party vendor router after the BGP authentication password is changed on the Cisco router.

  Workaround: Identify the BGP connection that is stale by entering the **show tcp brief** command and then clear the TCP control block.

- CSCsc39357

  Symptoms: A Cisco router may drop a TCP connection to a remote router.

  Conditions: This symptom is observed when an active TCP connection is established and when data is sent by the Cisco router to the remote router at a much faster rate than what the remote router can handle, causing the remote router to advertise a zero window. Subsequently, when the remote router reads the data, the window is re-opened and the new window is advertised. When this situation occurs, and when the Cisco router has saved data to TCP in order to be send to the remote router, the Cisco router may drop the TCP connection.

  Workaround: Increase the window size on both ends to alleviate the symptom to a certain extent. On the Cisco router, enter the **ip tcp window-size** *bytes* command. When you use a Telnet connection, reduce the *screen-length* argument in the **terminal length** *screen-length* command to 20 or 30 lines.

- 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.

Wide-Area Networking

- CSCec27942

  Symptoms: A virtual-access interface is not freed when a client session is torn down.

  Conditions: This symptom is observed on a Cisco router that is configured for VPDN when the client session is momentarily disconnected and then reconnected.

  Workaround: There is no workaround.

- CSCsh62833

  Symptoms: The **sessions per-mac throttle** command functions as expected, but when you enter the **show pppoe throttled mac** command, no output is displayed, and a warning message and traceback are generated:

  ```
  %SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header, chunk 0  data 70A48450
  chunkmagic 0  chunk_freema0
  -Process= "Exec", ipl= 0, pid= 234
  -Traceback= 6053AADC 606167A8 6158DB78 61578A28 61578B4C 604E4BF4 601C01E8
  604FE6F8 60617B54 60617B40
  604FE6F8  60617B54  60617B40
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that has an PRE-2, that runs Cisco IOS Release 12.2(28)SB4, and that is configured for PPPoE Connection Throttling. Note, however, that the symptom is not platform-specific.

  Workaround: There is no workaround.

- CSCsi08346

  Symptoms: Both accounting START and STOP records are not sent to a RADIUS server after an LNS failover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an LNS in a VPDN failover configuration with multihops and that is connected to a RADIUS server. The symptom occurs in a topology in which the LAC has access to both LNS platforms when the first LNS is not accessible but the second LNS is accessible.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(28)SB6

Cisco IOS Release 12.2(28)SB6 is a rebuild release for Cisco IOS Release 12.2(28)SB. This section describes a severity 3 caveat that is open in Cisco IOS Release 12.2(28)SB6. There are other open caveats in Cisco IOS Release 12.2(28)SB6. However, open caveats are normally listed only for maintenance releases, and the listing of CSCsg97961 is an exception.

Miscellaneous

- CSCsg97961

  Symptoms: A router may crash when you configure it with a high number of PPP over Ethernet over VLAN (PPPoEoVLAN) sessions that are spread over hundreds of VLAN subinterfaces.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2 or PRE-3.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(28)SB6

Cisco IOS Release 12.2(28)SB6 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(28)SB6 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCsc73699

  Symptoms: A router that is configured for NetFlow v9 may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(25)S4 or Release 12.2(27)SBC1 when the configuration is modified while the router actively exports flows. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- 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.

- CSCse68964

  Symptoms: When a PTA session is created with a traffic classifier (TC) service, the Parent-Session-ID attribute of the accounting packets of the TC service on the ISG does not match the Acct-Session-Id of the parent session after 16^2 (that is, 000000EE) Acct-Session-Ids have been used.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG and that is configured with QinQ subinterfaces over which PTA sessions are established.

Workaround: There is no workaround.

- CSCsf29098

  Symptoms: When you perform an OIR of a POS port adapter, a TLB Exception error may occur and the router may reset.

  Conditions: This symptom is observed on a Cisco router that has a POS port adapter with an interface that functions as an MPLS link in an AToM configuration when the POS interface has the **mpls ip** command enabled.

  Workaround: First disable the **mpls ip** command on the POS interface, then remove the AToM (Xconnect) configuration from the interface, and then perform an OIR of the POS port adapter.

- CSCsg48183

  Symptoms: A router may unexpectedly send an ARP request from all its active interfaces to the nexthop of the network of an SNMP server.

  Conditions: This symptom is observed on a Cisco router that has the **snmp-server host** command enabled after any of the following actions occur:

  - You reload the router.
  - A switchover of the active RP occurs.
  - You enter the **redundancy force-switchover main-cpu** command.

  Workaround: There is no workaround.

- CSCsg77508

  Symptoms: The parent session Accounting STOP record is missing RADIUS attributes 42, 43, 47 and 48.

  Conditions: This symptom is observed on a Cisco router that is configured to terminate a PPP over Ethernet over L2TP session when you apply a service policy to the session. The symptom occurs only when the session is configured with at least one traffic classification with per-flow accounting.

  When the PPP over Ethernet client is terminated, the RADIUS attributes 42,43, 47 and 48 are missing from the parent session Accounting STOP record.

  Workaround: There is no workaround.

EXEC and Configuration Parser

- CSCsc76550

  Symptoms: The RP may crash with a watchdog timeout error for the IP input process.

  Conditions: This symptom is observed on a Cisco router when you delete a subinterface that processes traffic.

  Workaround: Shut down the subinterface before you delete the subinterface.

IBM Connectivity

- CSCsf28840

  A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device.

There are workarounds available for this vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml.

IP Routing Protocols

- CSCed28542

  Symptoms: A router that is configured for PAT may generate the following error message and traceback while reporting slowness in the network:

  ```
  %SYS-2-INTSCHED: 'may_suspend' at level 3
  -Process= "IP NAT Ager", ipl= 3, pid= 118
  -Traceback= 80507F58 81310988 80CC14F8 80CD4F80 80CBAD30 80CBAD90 81321684 80CBB048
  80504118 805085E0
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.3(4)T and that has a high number (more than 2500) of NAT entries. The symptom is not release-specific.

  Workaround: There is no workaround.

- 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.

- CSCsg97662

  Symptoms: When you enter the **no ip nat service skinny tcp port 2000** command, NAT is not disabled on the 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.

Miscellaneous

- CSCef43197

  Symptoms: A router may crash when you enter the **no ip routing** command.

  Conditions: This symptom is observed on a Cisco router that has the **set ip next-hop** command enabled in a policy-based routing configuration and occurs when the router attempts to access freed adjacencies.

  Workaround: Remove the **set ip next-hop** command from the route map before you enter the **no ip routing** command.

- CSCei22697

  Symptoms: Some MVPN tunnels are mapped to an incorrect VRF forwarding table.

  Conditions: This symptom is observed on a Cisco router that is configured for data MDT groups.

  Workaround: There is no workaround.

- CSCei39688

  Symptoms: When a CEF initialization failure occurs, an ATM PVC that is configured for OAM may not pass traffic even though the PVC link status is up:

```
Router#show ip interface brief | include ATM
ATM3/0/0                   unassigned      YES manual up      up
ATM3/0/0.100               unassigned      YES unset  up      up
ATM3/0/0.300               10.1.1.1        YES manual up      up
ATM3/0/0.999               unassigned      YES unset  up      up

Router#show cef interface brief | include ATM
ATM3/0/0                        unassigned      up      dCEF
ATM3/0/0.100                    unassigned      down    dCEF
ATM3/0/0.300                    10.1.1.1        down    dCEF
ATM3/0/0.999                    unassigned      down    dCEF

Router#show ip cef | include 10.1.1.
10.1.1.0/30     attached             ATM3/0/0.300
```

  When CEF fails to initialize the ATM PVC, atm3/0/0.300, no /32 receive entries are created. Traffic that is destined for the IP address of the subinterface is dropped.

  Conditions: This symptom is observed on a Cisco router and occurs only when PAM is configured on the PVC.

  Workaround: To prevent the symptom from occurring, do not configure OAM on the PVC. When the symptom has occurred, enter the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected ATM subinterface. After the workaround has been applied, the output of the **show ip cef** command shows the following:

```
Router#show ip cef | include 10.1.1.
10.1.1.0/30     attached             ATM3/0/0.300
10.1.1.0/32     receive
10.1.1.1/32     receive
10.1.1.3/32     receive
```

- CSCek38382

  Symptoms: The standby PRE-2 crashes because of a debug exception, and the standby PRE-2 console shows the following error messages and traceback before the crash occurs:

```
%SYS-2-ASSERTION_FAILED: Assertion failed: "(*parents_ptr)->coll_magic ==
COLL_MAGIC_VAL"
-Process= "Deferred Adj Background", ipl= 0, pid= 167
-Traceback= 6050CA04 604AA1B4 60362364 60362510 603630A4 6035B67C 60360598 60FFAB30
60FF54A0 60FF5578
%Software-forced reload
```

  Conditions: This symptom is observed on a Cisco 10000 series after an ATM line card is reset.

  Workaround: There is no workaround.

- CSCek40657

  Symptoms: A PTA router may crash when you download a configuration with a class map, policy map, and PVC range to a point-to-point interface.

  Conditions: This symptom is observed on a Cisco 10000 series that functions as a PTA router.

  Workaround: There is no workaround.

- CSCek54106

  Symptoms: When you convert a non-queueing policy map to a queueing policy map and attach it to interfaces that do not support queuing, the QoS policy is removed from the interfaces and existing sessions.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Convert the non-queueing policy map to a queueing policy map before you apply it to interfaces or bring up sessions.

- CSCek54768

  Symptoms: E1 interfaces may go down when a line card is reset or removed even when the line card has APS enabled and an APS cutover is triggered. The interfaces do come back up within a few seconds.

  Conditions: This symptom is observed on a Cisco 10000 series that has a pair of 4-port channelized OC-3 line cards that are configured for SR-APS. The line cards are configured with E1 interfaces under either SONET or SDH.

  Workaround: Enter the **force** command in APS group configuration mode on both the router on which the line card is reset or removed and on the router at the far end to ensure that the line card that is reset or removed does not receive or transmit the active traffic.

  Note that the chances of the symptom occurring may be reduced when the line card that is reset or removed is not the active line card.

  Further Problem Description: This symptom occurs only when a line card is reset or removed, not when an APS switchover is triggered by a fiber cable that is removed.

  The symptom occurs because of a change in the E1 clock source that may occur when the line card is reset or removed and that causes alarms to be received. The symptom is more likely to occur when the line card has a large configuration and when the E1 interfaces are set to "clock source line."

- CSCek57646

  Symptoms: On a Cisco 10000 series, tracebacks and an error message that is related to the link index may be generated, and MLPoATM links continue to flap. The error message is similar to the following:

  ```
  %GENERAL-3-EREVENT: ttcm_add_mlp_member: 1926 No free link index available in
  Virtual-Access15
  ```

  Conditions: This symptom is observed when a member link of an MLPoATM bundle is modified.

  Workaround: There is no workaround.

- CSCek65046

  Symptoms: After a microcode reload has occurred, traffic is dropped for all users that have a per-user ACL configured and for which the user IP address is specified in the ACL.

  Conditions: This symptom is observed on a Cisco 10000 series when a per-user ACL is applied to each session and when an ACL Template is enabled.

  Workaround: After you have performed a microcode reload, disconnect and reconnect all sessions. Note that it is very likely that a user will reconnect a session after traffic has dropped.

- CSCir01277

  Symptoms: A Cisco 7304 may reload unexpectedly because of a watchdog reset condition, which can be seen in the output of the **show version** command.

  Conditions: This symptom is observed only on a Cisco 7304 that has an NPE-G100.

  Workaround: There is no workaround.

- CSCsa92748

  Symptoms: A Network Processing Engine G1 (NPE-G1) may restart unexpectedly and report the following message:

  ```
  Last reset from watchdog reset
  ```

  Conditions: This symptom is observed only on Cisco 7200 and Cisco 7301 series routers that are configured with an NPE-G1 Network Processing Engine.

  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.

- CSCsd08862

  Symptoms: A router may crash because of a bus error when you enter the **show interface** command or another command that displays the virtual-access information for a virtual-access interface or subinterface.

  Conditions: This symptom is observed while a session that is associated with the virtual-access interface or subinterface is being cleared.

  Workaround: There is no workaround.

- CSCsd19951

  Symptoms: When you attach a service policy to a POS interface and enter the **show policy-map interface** command, a spurious memory access and traceback are generated:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at 0x6184E5E8 reading 0x4
  %ALIGN-3-TRACE: -Traceback= 6184E5E8 6183E7C4 6184144C 6083B758 6083AF40 608416B4
  60841724 60841D80
  ```

  Conditions: This symptom is observed on a Cisco router only when a service policy has LLQ configured.

  Workaround: There is no workaround.

- CSCsd40153

  Symptoms: An ASBR has "No Label" as its outgoing label for a peer ASBR interface address.

  Conditions: This symptom is observed when the following conditions occur:

  - An ISP network (ISP network A) has two ASBRs that peer with one ASBR in another ISP network (ISP network B).
  - IGP routing (OSPF or any other IGP) is configured between the ASBRs in ISP network A.
  - A BGP session between one ASBR in ISP network A and the ASBR in ISP network B flaps.

  After about 5 minutes, all routes that are reachable via the ASBRs in ISP network A and the ASBR in ISP network B have "No Label" as their outgoing label.

  Workaround: Enter the **clear ip route** *network* command.

- CSCsd45936

  Symptoms: When a two-level hierarchical policy map in which the parent level has only a class default is already attached to an interface and when you configure a policer for both the parent and child levels, either of the following symptoms may occur:

  - When the child policy map is removed from the class default of the parent policy map, the traffic policing rate does not properly reflect the parent policer rate.
  - When the child policy map is attached to the class default of parent policy map, the traffic policing rate does not properly reflect the child policer rate.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB.

  Workaround: After the child policy is removed from or attached to the parent policy map, detach the policy map from the interface and re-attach it to the interface.

- CSCsd51309

  Symptoms: A platform may pause indefinitely or reload unexpectedly when you disable the MPLS Traffic Engineering AutoTunnel Mesh Groups feature.

  Conditions: This symptom is observed on a Cisco Catalyst 6500 series but is platform-independent.

  Workaround: There is no workaround.

- CSCse23232

  Symptoms: When a virtual template or user profile contains a service policy with class maps, the router may send not one but a number of RADIUS accounting-request packets for each PPPoE or PPPoEeoA session. The number of RADIUS accounting-request packets equals the number of class maps in the service policy. Each accounting-request packet has its own unique "acct- session-id."

  Conditions: This symptom is observed on a Cisco router that is configured with a QoS policy.

  Workaround: There is no workaround.

- 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.

  Workaround: There is no workaround.

- CSCse57312

  Symptoms: The MQC output policer does not add the L2 header as part of its calculation.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs only for multicast traffic on Ethernet and ATM interfaces.

  Workaround: There is no workaround.

- CSCse72235

  Symptoms: A Cisco 7200 series may crash because of an address error with corrupted program counter at "pc=0xAFACEFAD." This precise value is repeated in the traceback and in the "EPC," "BadVaddr," and "ra" registers. The crash may be preceded by a "%SYS-2-GETBUF: Bad getbuffer" error message.

Conditions: This symptom is observed on a Cisco 7200 VXR router that has an NPE-G1 and that runs Cisco IOS Release 12.2(28)SB2. The router is configured as a LAC with PPPoA and MPLS fragmentation for packets that travel from a PPPoA interface through an L2TP tunnel to an interface that is configured for MPLS.

Workaround: Disable MPLS.

Alternate Workaround: Disable fragmentation.

- CSCsf04423

  Symptoms: On a Cisco platform that is configured for MPLS and NetFlow, all traffic that leaves an interface may be process-switched, causing high CPU usage under the IP Input process. The symptom can be verified in the output of the **show interface statistic** command.

  Conditions: This symptom is observed when the **ip flow ingress** command is enabled on any interface on the platform and when MPLS is also enabled.

  Workaround: Enable MPLS-Aware NetFlow by entering the **ip flow-cache mpls label-positions** *label-position-1* command. Doing so prevents traffic from being process-switched, but note that additional MPLS fields are added to the NetFlow export records.

- CSCsf05044

  Symptoms: In a very large-scale MLPP configuration, that is, more than 300 MLP bundles, when a PRE-2 HA switchover occurs on a Cisco 10000 series, the following error message and/or a traceback may be generated on the connected Cisco 10000 series at the far end:

  ```
  ttcm_add_mlp_member: unable to install mlp link
  ```

  Conditions: This symptom is observed during the renegotiation of the links and line protocol of the interfaces and bundles.

  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.

- CSCsf19731

  Symptoms: The newly active PRE crashes immediately after an SSO switchover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series when an SSO switchover is triggered via SNMP.

  Workaround: Do not trigger an SSO switchover via SNMP. Rather use the CLI to trigger an SSO switchover.

- CSCsf27230

  Symptoms: When you configure a policy with WRED and shaping, random drops do not occur.

Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100.

Workaround: There is no workaround.

- CSCsf28159

  Symptoms: ISG accounting reports identical counter values for all services in the VSAs.

  Conditions: This symptom is observed on a Cisco router that functions as an ISG when the "accounting-list" is removed from the VSAs that are included in the request from the Cisco Subscriber Edge Services Manager (SESM).

  Workaround: Configure the SESM to include the "accounting-list" in the VSAs that are sent to the ISG.

- 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.

- CSCsf97199

  Symptoms: High CPU usage may occur during the "XDR mcast" and "XDR RP" background processes. Each of these processes uses more than 30 percent of the CPU while no data traffic passes through the router.

  Conditions: This symptom is observed on a Cisco 10000 series but is platform-independent.

  Workaround: Reload the router.

- CSCsg11718

  Symptoms: A VRF may become stuck in the "Delete Pending" state.

  Conditions: This symptom is observed on a Cisco router that is configured for MPLS VPN and Half-Duplex VRF (HDVRF) when you delete the VRF and then associate it with an interface before it is completely deleted.

  Workaround: To ensure that the VRF is properly deleted, enter the **shutdown** interface configuration command on the interface with which the VRF is associated or remove the interface with which the VRF is associated.

- CSCsg22981

  Symptoms: A router may crash because of a bus error when sending L2X data packets.

  Conditions: This symptom is observed on a Cisco 7301 that runs Cisco IOS Release 12.2(28)SB and that is configured for QoS. The symptom is platform-independent.

  Workaround: There is no workaround.

- CSCsg27043

  Symptoms: On a 7304 series Network Services Engine (NSE), the passing of packets from the PXF engine to the RP may freeze for a period from seconds to minutes. This situation causes the router to lose its routing protocol neighbors.

  Conditions: This symptom is observed rarely on a Cisco 7304 that runs Cisco IOS Release 12.2S or Release 12.2SB.

  Temporary Workaround: If the symptom occurs repeatedly, reloading the router may help.

- CSCsg29539

  Symptoms: In an MPLS core that carries EoMPLS traffic, an ingress PE router that has a TE tunnel to an egress PE router may stop sending EoMPLS traffic after the TE tunnel is rerouted across a different path in the MPLS core. When you enable the **debug mpls packet** command on the first P router in the topology, the debugs show that the EoMPLS packets enter with the wrong (that is, the old) TE tunnel label.

  Conditions: This symptom is observed on a Cisco 7304 that functions as a PE router and that runs Cisco IOS Release 12.2(28)SB or one of its rebuilds.

  Workaround: Clear the interface.

- CSCsg30757

  Symptoms: The following symptoms may occur for prepaid accounting:

  - There are no gigabit word attributes 52 and 53 for prepaid service, but when you enable the **debug radius** command, attributes 52 and 53 are shown for the parent session.
  - The prepaid service always sends the rollover counters in "I" and "O" as zero although the definitions are "I<HC>;<LC>" and "O<HC>;<LC>" in which HC indicates the rollover counter and LC indicates the lower 32 bit of the input and output octets counters.

  The following is part of the debugs and shows "I0;1963039136" and "O0;1963039136" and no attributes 52 and 53 ("gigaword rollover counters") although the amount of traffic over this service has exceeded the gigaword and has rolled over once already:

  ```
  RADIUS:   Cisco AVpair       [1]   36  "parent-session-id=0A0A440200000003"
  RADIUS:  Vendor, Cisco       [26]  21
  RADIUS:   ssg-control-info   [253] 15  "I0;1963039136"
  RADIUS:  Vendor, Cisco       [26]  21
  RADIUS:   ssg-control-info   [253] 15  "O0;1963039136"
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB and that is configured with a prepaid service policy.

  Workaround: There is no workaround.

- CSCsg31202

  Symptoms: A Cisco 7304 with an NSE-100 may crash and generate the following error message:

  ```
  Unexpected exception, CPU signal 10, PC = 0x4008B2EC
  ```

  Conditions: This symptom is observed very rarely when the router is configured with an input policy that marks incoming IP traffic on one interface and then uses this information for classification on an output policy on another interface.

  Workaround: There is no workaround.

- CSCsg35305

  Symptoms: A Cisco router that functions as an Intelligent Service Gateway (ISG) reloads when you enter the **show database** command.

  Conditions: This symptom is observed when existing sessions are in the process of being disconnected and when you enter the **show database** command for these sessions.

  Workaround: Do not enter the **show database** command for sessions that are in the process of being disconnected.

- CSCsg37423

  Symptoms: The output of the **show l2tun session l2tp** command does not include interface information.

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

Workaround: There is no workaround.

- CSCsg40949

  Symptoms: The PXF engine of a Cisco 10000 series may crash.

  Conditions: This symptom is observed rarely on a Cisco 10000 series when MLP is configured and when member links flap frequently.

  Workaround: There is no workaround.

- CSCsg64438

  Symptoms: When a prepaid service is unapplied from rules, the accounting stop record does not contain packet counts and octet counts.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) when the **service-policy type service unapply name** *policy-map-name* command (in which the *policy-map-name* argument indicates the prepaid service) is configured in the rules.

  Workaround for the packet counts: There is no workaround.

  Workaround for the octet counts: Look for the information in the following attributes that are present in the according stop record:

  ssg-control-info [253] 6 “I<high>;<low>” <low> indicates the input octets.

  ssg-control-info [253] 6 “O<high>;<low>” <low> indicates the output octets.

- CSCsg89189

  Symptoms: A router may reload when you enter the **show subscriber session detailed** command while sessions are being modified.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG).

  Workaround: Do not enter the **show subscriber session detailed** command while sessions are being modified.

- CSCsg93274

  Symptoms: When a switchover occurs on the standby PRE, the router does not sent a ciscoRFSwactNotif notification.

  Conditions: This symptom is observed on a Cisco 10000 series when the CISCO-RF-MIB traps are enabled for host that are configured to receive traps, that is, for valid SNMP hosts that have the **snmp-server enable traps rf** command enabled.

  Workaround: Configure SNMPv2 “informs.”

  Alternate Workaround: Use a static ARP configuration for the trap handlers that are configured via the **snmp-server host** command to increase the chances that the first few traps that are sent by the Cisco 10000 series are received by these trap handlers.

Wide-Area Networking

- CSCek55209

  Symptoms: When the **ppp multilink endpoint mac** *lan-interface* command or the **ppp multilink endpoint ip** *ip-address* command is configured, the router may unexpectedly reload if the multilink interface goes to the DOWN state, for example, when a PVC virtual circuit is unconfigured.

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

Workaround: There is no workaround. Do not use these configuration commands in Cisco IOS Releases 12.2SB, 12.3, and 12.4 without a fix for this DDTS.

- CSCek56250

  Symptoms: A router may reload while executing the **show ppp multilink** command.

  Conditions: This symptom is observed when a multilink bundle goes down while the output is being generated.

  Workaround: There is no workaround.

- CSCse66625

  Symptoms: A router does not accept the **pppoe max-sessions** *number* command on a subinterface.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB.

  Workaround: First configure the **pppoe max-sessions** *number* command on a BBA group, then attach this BBA group to the subinterface.

- CSCsg38412

  Symptoms: When a Multilink PPP (MLP) session is established over an ISDN link, IPCP fails to negotiate. When the **debug ppp negotiation** command is enabled, you can see that IPCP packets from the peer are not processed. The output of the **show interface** command for the ISDN D-channel interface shows that the input queue limit is 0.

  Conditions: This symptom is observed when the ISDN BRI or PRI interface is not configured as part of a dialer rotary group or dialer pool and when RADIUS is used to assign the multilink bundle to a VRF.

  Workaround: Enter the **dialer rotary-group** command to assign the ISDN interface to a dialer.

- CSCsg39977

  Symptoms: When dialer interfaces are used in conjunction with Multilink PPP (MLP), a router may crash because of a corrupted program counter.

  Conditions: This symptom is observed on a Cisco router when a dialer interface, including interfaces such as ISDN BRI and PRI interfaces, is configured to use MLP and when the queueing mode on the dialer interface is configured for Weighted Fair Queuing (WFQ). Note that WFQ is the default for some types of dialer interfaces.

  Workaround: There is no workaround.

- CSCsg56725

  Symptoms: When you enter the **terminate-from hostname** *host-name* command to terminate L2TP tunnels, some L2TP tunnels are terminated in the wrong VPDN group while other L2TP tunnels on the same host are terminated in the correct VPDN group.

  Conditions: This symptom is observed on a Cisco 7206VXR that has an NPE-G1 and that runs Cisco IOS Release 12.2SB and occurs only during the first two or three minutes after the router has booted. After that period, the symptom no longer occurs. Note that the symptom is platform-independent.

  Workaround: To prevent the symptom from occurring, enter the **no aaa accounting system guarantee-first** command on the router before you reload the router. Doing so enables the tunnels to be terminated in the correct VPDN groups.

  After the symptom has occurred, clear each of the affected tunnels by entering the **clear vpdn tunnel id** *local-id* command. Then, after the tunnels have been re-established, you should be able to terminate them in the correct VPDN groups.

Resolved Caveats—Cisco IOS Release 12.2(28)SB5

Cisco IOS Release 12.2(28)SB5 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(28)SB5 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCef29931

  Symptoms: When a Telnet connection to a router that is configured for secure login fails, memory corruption may occur on the router, and the router may reload.

  Conditions: This symptom is observed when the **login block-for** *seconds* **attempts** *tries* **within** *seconds* command is enabled on the router and when a user enters an incorrect password for the *tries* argument.

  When the Telnet connection fails, the router enters the quiet mode. When the router leaves the quiet mode, the router is able to accept Telnet connections. However, when the Telnet connections fails again, memory corruption occurs before the router enter the quite mode, and the router reloads.

  Workaround: There is no workaround.

- CSCeg52893

  Symptoms: Several tty lines may become stuck in the "Carrier Dropped" modem state. You can verify this situation by entering the **show line** *line-number* EXEC command for an individual line. However, when you enter the show line EXEC command (that is, you do not enter a value for the *line-number* argument), the output shows that the same tty lines are active (that is, they are in the "*" state):

  ```
  ......
  I   2/47 Digital modem - DialIn  -  -  -   7   0   0/0   -  Idle
  I   2/48 Digital modem - DialIn  -  -  -   7   0   0/0   -  Idle
  *   2/49 Digital modem - DialIn  -  -  -   5   0   0/0   -  Carrier Dropped
  I   2/50 Digital modem - DialIn  -  -  -   7   0   0/0   -  Idle
  I   2/51 Digital modem - DialIn  -  -  -  13   0   0/0   -  Idle
  I   2/52 Digital modem - DialIn  -  -  -  10   0   0/0   -  Idle
  ......
  ```

  In addition, both the output of the **show users** EXEC command and the output of the **show caller** EXEC command do not show a user or caller name or show an incorrect user or caller name. The output of the **show caller** EXEC command does show that the service is "TTY."

  Conditions: These symptoms are observed on a Cisco AS5400 that is configured for modem dial-in with PPP and EXEC connectivity and for login authentication via a TACACS+ server. The symptom is platform-independent.

  Workaround: To clear the stuck line, enter the **clear port** *slot*/*port* EXEC command.

- 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.

- CSCsc29669

  Symptoms: A bulk synchronization mismatch may occur when a switchover occurs on a Cisco 10000 series, or when you reload the router. This situation prevents the router from reaching the STANDBY HOT redundancy state in a timely manner.

  Conditions: This symptom is observed when you first define ann AAA attribute list and then force a switchover to occur. Just before the newly active PRE is supposed to enter the STANDBY HOT redundancy state, the following error messages are generated:

  ```
  Config Sync: Bulk-sync failure due to BEM mismatch. Please check the full list of BEM
  failures via:
    show issu config-sync failures bem
  Config Sync: Starting lines from BEM file:
    -aaa attribute list xxxxx
  ```

  Note that the symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCse09594

  Symptoms: A router crashes during the AAA authentication process for interfaces that are configured for PPP.

  Conditions: This symptom is observed on a Cisco router when the memory is exhausted. For example, the symptom may occur on a router that attempts to bring up more PPP sessions while its memory usage is already higher than 99 percent of the capacity because of existing configuration and sessions.

  Workaround: There is no workaround.

- CSCse70574

  Symptoms: RADIUS attributes for Acct-Input-Gigawords and Acct-Output-Gigawords counters are not present in per-service accounting on an ISG. Octets counters overflow, but the Gigawords attributes are not included in the accounting records for the service, preventing the RADIUS billing server from being notified that the input and output counters have rolled over.

  Conditions: This symptom is observed on a Cisco 10000 that runs Cisco IOS Release 12.2(28)SB2 and that functions as an ISG. The symptom may be platform-independent.

  Workaround: There is no workaround.

  Further Problem Description: RADIUS attributes for Acct-Input-Gigawords and Acct-Output-Gigawords counters are being counted and function properly for parent PPP sessions on an ISG.

Interfaces and Bridging

- CSCsa87986

  Symptoms: A router may intermittently transmit corrupt PPP packets. When you enter the **debug ppp nego** and **debug ppp errors** commands, it appears that “protocol reject” packets are received from the remote end.

  Conditions: This symptom is observed on a Cisco 7500 series that has only one OC-3 POS port adaptor per VIP and that is configured for PPP encapsulation.

  Workaround: Configure an outbound policy on the interfaces of the OC-3 POS port adaptors.

IP Routing Protocols

- 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.

- CSCeh49504

  Symptoms: BGP redistribution into EIGRP based on a standard community or AS path does not work as expected.

  Conditions: This symptom is observed when the **match community** or **match as-path** route-map commands are enabled.

  Workaround: There are two steps to this workaround:

  1. Apply an inbound route map on the BGP neighbor. The inbound route map must include the **set metric** command to set the BGP multi-exit discriminator (MED) based on the standard community or AS path.
  2. Match on the BGP MED in the route map that is used in the BGP redistribution.

  Further Problem Description: Set actions in one particular statement that includes the **match community** or **match as-path** command are applied to all routes that match any subsequent statement in the same route map, instead of only to the routes that match the particular statement to which the set actions were applied.

- CSCei77227

  Symptoms: A Cisco router that functions in a multicast VPN environment may crash.

  Conditions: This symptom is observed when you check the unicast connectivity and then unconfigure a VRF instance.

  Workaround: There is no workaround.

- CSCek33991

  Symptoms: A router may reset unexpectedly when it is in the midst of output of the results of the **show interface dampening** command, and the interface is deleted from another vty connection.

  Conditions: This symptom can be encountered if concurrent connections are opened to a router, and the **show interface dampening** command is issued while interface(s) are deleted.

  Workaround: Ensure interfaces with **dampening** configured are not deleted while the **show interface dampening** command can be possibly issued on another vty.

- 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.

- CSCsb09852

  Symptoms: The number of networks in the BGP table and the number of attributes increases, and a slower convergence may occur for members of a BGP update group.

  Conditions: This symptom is observed on a Cisco router when the members of a BGP update group go out of synchronization with each other in such a way that they have different table versions, preventing the BGP Scanner from freeing networks that do not have a path.

  To check if the members of the BGP update group are in synchronization with each other, enter the **show ip bgp update-group summary** command and look at the table version for each member. If they have the same table version, they are in synchronization with each other; if they do not, they are out of synchronization with each other.

  Workaround: To enable the members of the BGP update group to synchronize with each other, enter the **clear ip bgp * soft out** command. Doing so does not bounce the sessions but forces BGP to re-advertise all prefixes to each member.

- CSCsb36755

  Symptoms: When BGP receives an update that has a worse metric route than the previously received route for equal-cost multipath, the BGP table is updated correctly but the routing table is not, preventing the old path from being deleted from the routing table.

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

  Workaround: Enter the **clear ip route** *network* command.

- CSCsb50606

  Symptoms: Memory utilization 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.

- 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.

- CSCsd59023

  Symptoms: ARP entries that are associated with the default interface (of the default route or network) are refreshed when they should not be refreshed.

  Conditions: This symptom is observed on a Cisco router when other interfaces change their state or when the IP configuration of other interfaces is changed.

  Workaround: There is no workaround.

- CSCsd67591

  Symptoms: A router may crash when you modify parameters of the **route-map** command for a redistribution statement.

  Conditions: This symptom is observed when you modify the parameters of the **route-map** command for a redistribution statement of an OSPF process that was deleted.

  Workaround: Delete the redistribution statement before you delete the OSPF process.

- CSCse41600

  Symptoms: A router may crash when VRFs and BGP configurations are removed quickly.

  Conditions: This symptom is observed on a Cisco router that has many VRFs and BGP configurations.

  Workaround: Remove the VRFs and BGP configurations slowly to avoid timing issues.

- CSCse51629

  Symptoms: A router may crash when use the **copy tftp:** *filename* **system:running-config** command for bulk unconfiguration of subinterfaces.

  Conditions: This symptom is observed on a Cisco router that has a large number of PVCs (that is, more than 200) and many subinterfaces, that is configured for OSPF, and that is processing traffic from 40,000 IP source addresses.

  Workaround: Do not use the **copy tftp:** *filename* **system:running-config** command for bulk unconfiguration of subinterfaces.

- 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.

- 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.

Miscellaneous

- CSCeb80947

  Symptoms: Disconnecting VPDN users via the CISCO-AAA-SESSION-MIB does not work.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(13)T or a later release of Release 12.2T. The symptom may also occur in other Cisco IOS software release trains.

  Workaround: There is no workaround.

- CSCeg26728

  Symptoms: BGP may fail to establish a peer with another router when an output service policy is configured on an interface and the output service policy limits the bandwidth to 199 kbps for packets that have the IP precedence value set to 6.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2(14)S9. However, the symptom is not platform- and release-specific.

  Workaround: Remove the output service policy from the interface.

- CSCei38741

  Symptoms: Tracebacks are generated on a Cisco 10000 series that is configured with serial interfaces.

  Conditions: This symptom is observed when you change the encapsulation on a serial interface from PPP to Frame Relay.

  Workaround: Before you change the encapsulation from PPP to Frame Relay, enter the **no encapsulation ppp** command.

- CSCei80699

  Symptoms: Duplicate Interface Index (ifIndex) numbers may be assigned to the multicast tunnel interfaces. This situation may prevent traffic from being switched from these multicast interfaces, and may cause the router to crash with a bus error when these multicast tunnels are deleted and then re-created.

  You can verify that the symptom has occurred by entering the **show idb** command and by looking for duplicate ifIndex entries for the multicast tunnel interfaces.

  Conditions: This symptom is observed on a Cisco router that is configured with PIM and MDT multicast tunnels.

  Workaround: There is no workaround.

- CSCej87817

  Symptoms: Policing does not drop any packets after the packets are sent or received at a rate that is much higher than the committed information rate (CIR).

  Conditions: This symptom is observed on a Cisco 7500 series router but is not platform dependent.

  Workaround: There is no workaround.

- CSCek25192

  Symptoms: When you configure traffic policing in percentages, the following error message floods the console:

  ```
  Maximum rate for the policer is 0. Conform action is drop.
  ```

  Conditions: This symptom is observed on a Cisco router that is configured for Control Plane Policing (CoPP).

Workaround: There is no workaround.

- CSCek27377

  Symptoms: A Cisco 7304 that is configured for QoS may reload unexpectedly.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 when you apply or remove a policy map on an egress interface and occurs only when the policy map invalidly has a **shape** command at both the parent and child levels.

  Workaround: There is no workaround.

- CSCek32110

  Symptoms: A Cisco 7304 may crash because of a bus error when you perform an OIR of an ATM line card while traffic is passing through the line card.

  Conditions: This symptom is observed when the ATM line card is configured with many VCs and when traffic is switched while the PXF engine is disabled.

  Workaround: There is no workaround.

- CSCek33894

  Symptoms: When an HA switchover occurs, the standby RP resets continuously.

  Conditions: This symptom is observed on a Cisco router that functions as an Intelligent Service Gateway (ISG) when service policy maps access traffic class maps.

  Workaround: There is no workaround.

- CSCek40192

  Symptoms: Traffic convergence takes more than 50 ms after an Automatic Protection Switching (APS) switchover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCek42178

  Symptoms: An APS switchover does not occur at the far end when you enter the **hw-module slot reset** command at the near end.

  Conditions: This symptom is observed on a Cisco 10000 series

  Workaround: There is no workaround.

- CSCek42422

  Symptoms: SNMP MIB entries for the following GBIC/SFPs are missing from Cisco OS Release 12.2(28)SB and later releases:

  - CWDM-1470
  - CWDM-1490
  - CWDM-1510
  - CWDM-1530
  - CWDM-1550
  - CWDM-1570
  - CWDM-1590
  - CWDM-1610

Conditions: This symptom is observed on a Cisco 7304 when you issue a SNMP Get command for the ENTITY-MIB.

Workaround: There is no workaround.

- CSCek43620

  Symptoms: A bulk synchronization may fail because of a “best-effort method” mismatch, causing the standby PRE to reset unexpectedly.

  Conditions: This symptom is observed on a Cisco 10000 series when APS is configured for an ATM line card and when one or more ports are administratively down.

  Workaround: Either remove the APS configuration from the ATM line card or bring up all the ports by entering the **no shutdown** interface configuration command before the standby PRE is loaded. Then, after the standby PRE has loaded, you may return the port(s) to the administratively down state.

- CSCek46087

  Symptoms: Interprocessor communication within line cards that are installed in a router chassis may not function properly.

  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.

  Workaround: There is no workaround.

- CSCek47252

  Symptoms: A Cisco 7304 may reload unexpectedly when you enter the **show diag** *slot-number* command for a Port Adapter Carrier Card (7300-CC-PA).

  Conditions: This symptom is observed rarely on a Cisco 7304 and occurs only when the **show diag** *slot-number* command causes the 7300-CC-PA to reset unexpectedly.

  Workaround: To prevent the symptom from occurring, do not enter the **show diag** *slot-number* command or the **show tech-support** command, which includes the **show diag** *slot-number* command.

- CSCek49488

  Symptoms: When a Cisco IOS software image is loaded onto a Cisco 7304 that has a Port Adapter Carrier Card (7300-CC-PA), the error messages similar to the following may be generated and the 7300-CC-PA may reload unexpectedly:

  ```
  %LC-3-LCI2C_ERROR: PA Carrier Card Linecard I2C bus access failed at slot 4, status
  = 0x1
  -Traceback= 4056860C 407A2D10 4072F8C0 40737FE8 406DC95C 4066A304

  %LC-3-CLFPGAERROR: Line card common logic fpga (slot 4) error: Egress data fifo
  controller error

  %LC-3-CLFPGAERROR: Line card common logic fpga (slot 4) error: Bad control code
  (0x8888) from egress data port o

  %LC-3-RECOVERY: Line card (slot 4) recovery in progress
  -Traceback= 4056860C 407310F0 407388D0 401F38E8 40736F48 407373D8 406D3498 406268B4
  4056FEDC 40570270 40648F04 40648EF0

  %LC-6-VIRTUALINIT: Line card (slot 4) - initialization in virtual mode
  ```

  The same symptom may occur when you enter the **hw-module slot** *slot-number* **stop** command followed by the **hw-module slot** *slot-number* **start** command to stop and restart the 7300-CC-PA.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(28)SB, 12.2(28)SB1, 12.2(28)SB2, 12.2(28)SB3, or 12.2(28)SB4.

  Workaround: There is no workaround. However, the 7300-CC-PA recovers automatically.

- CSCek49580

  Symptoms: The configuration may become lost, the standby PRE may crash, the active PRE may crash, and other problems may occur.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for RPR+ when you enter the **bert t3** command from the controller menu or when you abort the **bert t1** command during execution.

  Workaround: Only enter the **bert t3** command from the interface menu, and do not abort the **bert t1** command during execution.

- CSCek51309

  Symptoms: A router may reload when a QoS policy is attached to a number of PPPoL2TP sessions on an LNS and when the physical link or sessions are flapping. The QoS policy contains a shaping and queuing configuration.

  Conditions: This symptom is observed on a Cisco router that functions as an LNS when there are many route changes, either because a physical interface flaps or because the PPPoL2TP sessions flap.

  Workaround: There is no workaround.

  Further Problem Description: The symptoms are specific to L2TP sessions and queuing features in the policy map.

- CSCek52915

  Symptoms: A router may lock up and all forwarding may stop after a priority statement is first removed and then returned into an LLQ policy map.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with 100 ATM VCs and that processes voice and data traffic.

  Workaround: There is no workaround.

- CSCek57494

  Symptoms: All packets may be dropped across a T1 or E1 link on which class-based shaping is configured.

  Conditions: This symptom is observed on a Cisco 7200 series that has an NPE-G1 and that runs Cisco IOS Release 12.2(28)SB.

  Workaround: There is no workaround.

- CSCin99687

  Symptoms: An SNMP walk of the dsx1IntervalTable results in an infinite loop.

  Conditions: This symptom is observed on a Cisco router that is configured with a PA-MCX-8TE1 or PA-MC-2T3+ port adapter.

  Workaround: There is no workaround.

- CSCin99753

  Symptoms: When you enter the **test pppoe** command on the PPPoE client, the PPPoE client or PPPoE server crashes.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that functions as a PPPoE client or PPPoE server. When the Cisco 7304 functions as a server and you enter the **test pppoe** command on another Cisco 7304 that functions as a PPPoE client, the PPPoE server crashes. When another router functions as the PPPoE server and a Cisco 7304 functions as the PPPoE client, the PPPoE client crashes.

Workaround: There is no workaround.

- CSCir00106

  Symptoms: IPC timeout messages may be generated on a Cisco 7304 that has an NSE-100.

  Conditions: This symptom is observed when the CPU usage of the router is at 100 percent, when the PXF engine is switched off, and when there is a heavy traffic that is punted to the RP.

  Workaround: Enable PXF switching by entering the **ip pxf** command.

- 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.

  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.

- CSCsc42938

  Symptoms: A router that is configured for Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) may crash when LDP is configured globally or on an interface.

  Conditions: This symptom is observed when you enter the **show mpls ldp neighbor** command while LDP sessions are coming up or going down.

  Workaround: There is no workaround.

- CSCsc60242

  Symptoms: ATM subinterfaces may flap unexpectedly and cause the routing protocol neighbor to flap.

  Conditions: This symptom is observed on a Cisco 10000 series that has a PRE-2 and occurs when the OAM queue depth is not set correctly.

  Workaround: There is no workaround.

- CSCsd11815

  Symptoms: The **random-detect precedence** *precedence min-threshold max-threshold* Interface is not accepted. This situation prevents the packets that match the value of *precedence* argument from being dropped.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCsd15575

  Symptoms: Packets are not forwarded via a GRE tunnel.

Conditions: This symptom is observed on a Cisco 10000 series when you enter the **no service pxf** command.

Workaround: Do not disable the PXF engine.

- CSCsd44362

  Symptoms: After a switchover has occurred, a watchdog timeout crash that occurs because of a CPUHOG condition may prevent the secondary RP from becoming the primary RP.

  Conditions: This symptom is observed on a Cisco 7304 when a few OIRs are performed before the switchover occurs. The router has an ATM line card on which a few PVCs are configured.

  Workaround: There is no workaround. However, after the watchdog timeout crash gas occurred, the secondary RP comes up as the primary RP.

- CSCsd45416

  Symptoms: An interface on a SPA-2GE-7304 or SPA-4FE-7304 may become stuck after a few HA switchovers have occurred.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCsd56598

  Symptoms: When a switchover occurs, an interface remains down.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for SSO when the following events occur:

  1. You remove a port adapter or line card via an OIR.
  2. An SSO switchover occurs.
  3. You insert the port adapter or line card via an OIR.

  After these events, the interface remains down.

  Workaround: There is no workaround.

- CSCsd73865

  Symptoms: When you log off from a service, a router may generate the following error message and then crash:

  ```
  %SW_MGR-3-CM_ERROR: Connection Manager Error - unprovision segment failed
  [ADJ:TC:61470] - hardware platform error.
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that functions as an ISG when you first change a locally defined service profile, then activate the service, and then log off from the service.

  After you have activated the service, the output of the **show subscriber session all** command indicates that the service has both previously applied profile features and currently applied profile features.

  Workaround: There is no workaround.

- CSCsd82072

  Symptoms: A CPUHOG error message and tracebacks may be generated on a Cisco 10000 series.

  Conditions: This symptom is observed when a 4-port channelized T3 half-height comes up with a large configuration.

  Workaround: There is no workaround.

- CSCsd98739

  Symptoms: The policer stops functioning when you remove classes for which no police action is configured and when these classes are defined before a class that does have a police action configured.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Remove and re-apply the service policy to the affected interfaces.

- CSCse11694

  Symptoms: When you bring up ISG sessions with the L4 Redirect feature under a high traffic load, translations may not be successfully created for all ISG sessions.

  Conditions: This symptom is observed on a Cisco router when you bring up more than 8000 ISG sessions and send IP packets at 4800 pps.

  Workaround: There is no workaround.

- CSCse16519

  Symptoms: A service policy is not applied to LAC sessions.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2SB and that functions as a LAC.

  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.

- CSCse26583

  Symptoms: When you enter the **shape average percent** *percentage* command to change a shaper policy with a shaper rate in bits per second (bps) to a shaper rate in percentage, the rate change is not reflected properly.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs with any type of policy (that is, with a single-level policy without a child policy or a two-level policy with a child policy attached to the parent policy and with a user-class or a class-default class).

  Workaround: Remove and re-attach the policy.

  Further Problem Description: The following changes in the shaper rate are not affected:

  - percentage to percentage
  - bps to bps
  - percentage to bps

- 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.

  Workaround: There is no workaround.

- CSCse28363

  Symptoms: A Cisco 10000 series may crash when you remove a POS interface.

  Conditions: This symptom is observed on a Cisco 10000 series when you enter the **shutdown** interface configuration command an interface of a 1-port OC-12 POS line card.

  Workaround: There is no workaround.

- CSCse29953

  Symptoms: When a large number of PPPoE sessions come up on a Cisco 10000 series that functions as an LNS, some formerly established sessions may disconnect.

  Conditions: This symptom is observed on a Cisco 10000 series when the number of sessions approaches or exceeds 50,000 and when a keepalive value is set on the virtual template that is applied to the tunnel. This symptom occurs when the CPU usage is high while the PPPoE sessions are brought up.

  Workaround: Enter the **no keepalive** command on the virtual template that is applied to the tunnel.

  Further Problem Description: PPP keepalive timeouts cause the PPPoE sessions to disconnect because they time-out prematurely.

- CSCse30164

  Symptoms: The environment monitor checksum value in the IDPROM of a 4-port 10/100 Fast Ethernet SPA (SPA-4FE-7304) is incorrect.

  Conditions: This symptom is observed on a Cisco 7304 and is specific to the SPA-4FE-7304.

  Workaround: There is no workaround.

- CSCse34799

  Symptoms: Are router that processes Label Distribution Protocol (LDP) traffic for a sustained period of time may generate the following error messages and tracebacks, and the CPU usage may become high:

  ```
  %GENERAL-3-EREVENT: HWCEF: Failed to allocate HW mac rewrite
  -Traceback=
  ```

  ```
  %GENERAL-2-CRITEVENT: Bad RP 2 XCM address conversion
  -Traceback=
  ```

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for MPLS and LDP when continuous LDP link flapping occurs.

  Workaround: There is no workaround.

- CSCse37573

  Symptoms: The NPE-G100 in a Cisco 7304 crashes after the PA-CC has crashed.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S10 or Release 12.2SB and that is configured with a PA-CC in which an 8-port ATM IMA port adapter is installed.

  Workaround: There is no workaround.

- CSCse37614

  Symptoms: Qos preclassification on a GRE tunnel may not function.

  Conditions: This symptom is observed on a Cisco 7200 series and a Cisco 7304 that has an NPE-G100.

  Workaround: There is no workaround.

- CSCse49552

  Symptoms: ATM ports may stop sending and receiving traffic when the ATM VCs are no longer synchronized between the Cisco IOS software and the ATM line card.

  Conditions: This symptom is observed on a Cisco 10000 series when an MTU change or a hold-queue length change cause the SAR of the ATM line card to reset.

  Workaround: There is no workaround to prevent the symptom from occurring. After the symptom has occurred, enter the no shutdown command on all ATM ports or reset the ATM line card by entering the **hw-module slot** *slot-number* **reset** command to enable the ATM VCs on multiple ports to synchronize properly between the Cisco IOS software and the ATM line card.

- CSCse54482

  Symptoms: A parser error and configuration synchronization error may occur when you enter a **banner** command that contains a carriage return. This situation causes the standby NSE-100 to fall back to RPR mode.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(28)SB or Release 12.2(28)SB1 and that has dual NSE-100 processors that function in SSO mode.

  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.

- CSCse62630

  Symptoms: When L2VPN circuits (that is, either AToM or L2TPv3 circuits) are configured for Ethernet interworking on an NSE-100, loss of connectivity may occur.

  Conditions: This symptom is observed on a Cisco 7304 and occurs only when there are more than 255 L2VPN circuits configured.

  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.

- CSCse73032

  Symptoms: Multicast routes fail, CEF routes fail, NAT translations fail, MPLS routes over an EtherChannel fail, or the router reloads unexpectedly.

  Conditions: These symptoms are observed on a Cisco 7304 that has an NSE-100 processor that runs Cisco IOS 12.2(25)S or a rebuild of this release up to and including Release 12.2(25)S10. The symptoms occurs under stress conditions when NAT and multicast are used (but not necessarily for the same traffic flows).

  In Release 12.2(28)SB or one of its rebuilds, the symptoms may occur when a Cisco 7304 that has an NSE-100 processor functions under stress conditions and when the following combinations of features are in use (but not necessarily for the same traffic flows):

  - NAT and multicast
  - MPLS over EtherChannel and large CEF tables
  - Multicast and large CEF tables

  Workaround: Disable PXF. If this is not an option, there is no workaround.

- CSCse78349

  Symptoms: A Cisco 7304 that is configured for multicast may drop packets from its PXF engine.

  Conditions: This symptom is observed only on a Cisco 7304 that has an NSE-100 and occurs when the router is at the transition of the sparse-mode and dense-mode regions and when the following events take place:

  1. A stream from the dense-mode side halts, causing the (s,g) entry to time out.
  2. The stream restarts before the corresponding (*,g) entry times out.

  This situation causes the packets to be dropped from the PXF engine and occurs because the output list interface for the (*,g) entry points toward the source in the dense-mode region.

  Workaround: Enter the **no ip mroute-cache** command on the input interface in dense mode.

- 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.

- CSCse85435

  Symptoms: A temporary loss of connectivity may occur on a 4-port channelized T3 half-height line card. The line card recovers automatically in 10 to 20 seconds for a small configuration, or potentially a longer time for very large configuration. For a small configuration without Frame Relay connections, the loss of connectivity may not even cause a line flap.

  Conditions: This symptom is observed on a Cisco 10000 series immediately after an SSO switchover has occurred. The symptom can occur with both a PRE-2 and a PRE-3.

  Workaround: There is no workaround.

- CSCse98421

  Symptoms: When a Cisco 7304 that functions in an MPLS environment as a P router receives MPLS traffic that is forwarded as pure IP traffic, the router may incorrectly apply an MPLS string rather than an IP string, causing the next PE router to drop packets that have a size larger than 1496 bytes.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100, that runs Cisco IOS Release 12.2(28)SB1 or Release 12.2(28)SB2, that has PXF enabled, and that has MPLS configured on the connecting interfaces.

  Workaround: Disable PXF, downgrade to Cisco IOS Release 12.2(25)S8, or disable MPLS. However, if none of these solutions is an option, there is no workaround.

  Further Problem Description: The same symptom is observed irrespective of the FPGA microcode that is used. The connecting interfaces have the **mtu 1512** and **ip mtu 1500** commands enabled so the MPLS MTU is the same as the interface MTU and the IP MTU is a bit less than the interface MTU to accommodate for two labels.

- CSCsf03188

  Symptoms: A router crashes when you use TFTP to download a configuration to the running configuration and when the downloaded configuration clears the controllers.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsf08287

  Symptoms: After a PRE failover as occurred, the Multi-Router APS (MR-APS) state is mismatched between the active PRE and the standby PRE.

  Conditions: This symptom is observed on a Cisco 10000 series when the PREs function in SSO mode and when a 1-port OC-12 ATM line card or 4-port OC-3 ATM line card is connected to an ADM and is configured for MR-APS.

  Workaround: There is no workaround.

- CSCsf19377

  Symptoms: A Cisco 10000 series that is configured for MPLS AToM may crash.

  Conditions: This symptom is observed on a Cisco 10000 series that runs Cisco IOS Release 12.2(31)SB.

  Workaround: There is no workaround.

- CSCsf26075

  Symptoms: When a service policy with random-detect is attached to a physical interface, the logical subinterfaces may ignore the policy.

  Conditions: This symptom is observed only on a Cisco 7304 that has an NSE-100. The physical interfaces that are affected are Ethernet and Frame Relay interfaces. For example, when there is an interface with two Frame Relay virtual circuits and a service policy with random-detect on the main interface, then none of the traffic that passes through the VCs is subjected to WRED.

  Workaround: There is no workaround.

- CSCsg06445

  Symptoms: A PRE-2 may crash because of an “Illegal Opcode” exception.

  Conditions: This symptom is observed rarely on a Cisco 10000 series that functions as an LNS that processes L2TP traffic.

  Workaround: There is no workaround.

- CSCsg07004

  Symptoms: IP header compression does not function. The output of the **show ip tcp header compression** command shows that no frames have been compressed.

  Conditions: This symptom is observed on a Cisco 7304 with an NPE-G100 when CEF is enabled on the interface on which header compression is also enabled.

  Workaround: Disable CEF on the interface on which header compression is enabled.

Wide-Area Networking

- CSCeg82698

  Symptoms: PPTP tunnels do not come up.

  Conditions: This symptom is observed when VPDN is configured.

  Workaround: There is no workaround.

- CSCek31721

  Symptoms: A router may not release the memory when sessions are freed. This situation may prevent PPP interfaces from coming up or initializing.

  Conditions: This symptom is observed on a Cisco router that is configured for HA when PPP interfaces flap.

  Workaround: There is no workaround.

- CSCek39651

  Symptoms: A TERMREQ packet that is sent from an LNS may not reach a PPP client, causing the PPP client connection to be disconnected because of a “missed keepalives” or “lower layer disconnected” message instead of a “peer disconnected” message.

  Conditions: This symptom is observed on a Cisco router that functions as an LNS when a PPP call that is forwarded over an L2TP or L2F VPDN tunnel is disconnected at the LNS.

  Workaround: There is no workaround.

- CSCek40618

  Symptoms: A router may crash by address error (load or instruction fetch) exception during normal operation.

  Conditions: This symptom has been observed when the router is configured with VPDN and Multilink PPP, using Virtual-Template interfaces.

  Workaround: There is no workaround.

- CSCsd01816

  Symptoms: Multilink interfaces do not recover after a T1 link in a bundle flaps.

  Conditions: This symptom is observed when two Cisco router are connected back-to-back via two channelized OC-3 connections with 168 T1 links and when the multilink bundles are created with two T1 links each.

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

- CSCsd44299

  Symptoms: Tracebacks may be generated when you change the MTU size of a bundle link on a physical serial interface. After you have reloaded or power-cycled the router, the tracebacks continue to be generated. The router crashes when you remove the **frame-relay fragment** *fragment-size* **end-to-end** command from the MFR interface.

  Conditions: These symptoms are observed on a Cisco 7200 series that runs Cisco IOS Release 12.2SB and occurs only for MFR interfaces that have interface-level FRF.12 fragmentation enabled.

  Workaround: Do not configure interface-level FRF.12 fragmentation. Rather, configure FRF.12 fragmentation in a map class with traffic shaping.

- CSCsd75377

  Symptoms: PPP links may not come up after an RPR+ switchover has occurred. You can compare the output of the **show ip interface brief | in up down** command before and after the RPR+ switchover to see which PPP interfaces are down.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for RPR+ but may also occur other platforms that are configured for RPR+.

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

- CSCse40960

  Symptoms: PPP keepalives may be processed at the process level (that is, in the slow path), and LCP negotiation may fail, causing links to flap repeatedly.

  Conditions: This symptom is observed on a Cisco 10000 series that has PPP keepalives enabled. However, the symptom may be platform-independent.

  Workaround: There is no workaround.

- CSCse70647

  Symptoms: A router that functions as a BRAS or LNS crashes and generates one of the following error messages (or an error message that is similar to one of the following error messages):

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x607C0374
  ```

  or

  ```
  %SYS-2-CHUNKFREE: Attempted to free nonchunk memory, chunk 206BCF18, data 21CD607D.
  -Process= "PPPoA Manager", ipl= 0, pid= 220
  ```

  or

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

  Conditions: This symptom is observed during PPP negotiations with a Microsoft PPP client that requests WINS or DNS data. Note that the symptom does not occur on a router that functions as a LAC.

  Workaround: There is no workaround. However, entering the **ppp max-failure 100** command may reduce the chances that the symptom occurs.

- CSCse81359

  Symptoms: After you have shut down a Frame Relay over MPLS (FRoMPLS) connection, the **xconnect** command is unexpectedly removed from the standby PRE, preventing the FRoMPLS connection from coming up after an HA switchover has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series.

Workaround: When you enter the **connect** command on the active PRE, also enter the **xconnect** command and any other configuration from the connect submode on the standby PRE to ensure that the complete configuration is retained on the standby PRE after an HA switchover has occurred.

- CSCse96387

  Symptoms: In a large scale Broadband Access Aggregation (BBA) environment, PPP negotiation may become stuck in a state in which one side is closed and the other side is constantly attempting to request options. This situation may cause all sessions to become stuck in a bad state that you must manually clear in order to recover from the state.

  Conditions: This symptom is observed on a Cisco router when a large volume of sessions comes up all at once as is common in an PPPoA BBA environment.

  Workaround: If you think you are encountering this caveat, please contact Cisco Technical Support Services for assistance and possible configuration tuning to minimize the chance that the symptom occurs again.

  Further Problem Description: If this is an option for your configuration, you can also reduce the rate of the incoming sessions to minimize the chance that the symptom occurs again.

- CSCse98867

  Symptoms: A router may reload when a multilink bundle goes down while packets are flowing.

  Conditions: This symptom is observed on a router that is configured for Multilink PPP (MLP) with hardware compression.

  Workaround: There is no workaround.

- CSCsf98296

  Symptoms: PPP keepalives fail because there are an extra 4 bytes added to an LCP echo reply.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBB or Release 12.2(28)SB. The symptom occurs when the Cisco router is connected to certain third-party vendor routers that strictly validate the received echo replies; the Cisco router adds an extra 4 bytes to the echo replies, causing them to be ignored by the third-party vendor routers.

  Workaround: Disable keepalives on the third-party vendor routers. If this is not an option, there is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(28)SB4

Cisco IOS Release 12.2(28)SB4 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(28)SB4 but may be open in previous Cisco IOS releases.

EXEC and Configuration Parser

- CSCsd72511

  Symptoms: When TACACS+ command accounting is enabled, SNMPv3 community strings may not be encrypted.

  Conditions: This symptom is observed on a Cisco platform that runs Cisco IOS Release 12.2.(25)SEE. The symptom also affects other releases.

  Workaround: There is no workaround.

Miscellaneous

- CSCek51309

  Symptoms: A router may reload when a QoS policy is attached to a number of PPPoL2TP sessions on an LNS and when the physical link or sessions are flapping. The QoS policy contains a shaping and queuing configuration.

  Conditions: This symptom is observed on a Cisco router that functions as an LNS when there are many route changes, either because a physical interface flaps or because the PPPoL2TP sessions flap.

  Workaround: There is no workaround.

  Further Problem Description: The symptoms are specific to L2TP sessions and queuing features in the policy map.

- CSCse71784

  Symptoms: When you configure an IP address as the tunnel source and the tunnel interface has been disconnected, shut down, or reconfigured, the tunnel interface line protocol can no longer come up.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(25)S or Release 12.2SB.

  Workaround: Do not configure an IP address as the tunnel source. Rather, at both ends of the tunnel, configure the source interface or the interface name as the tunnel source.

- CSCsf04754

  Multiple Cisco products contain either of two authentication vulnerabilities in the Simple Network Management Protocol version 3 (SNMPv3) feature. These vulnerabilities can be exploited when processing a malformed SNMPv3 message. These vulnerabilities could allow the disclosure of network information or may enable an attacker to perform configuration changes to vulnerable devices. The SNMP server is an optional service that is disabled by default. Only SNMPv3 is impacted by these vulnerabilities. Workarounds are available for mitigating the impact of the vulnerabilities described in this document.

  The United States Computer Emergency Response Team (US-CERT) has assigned Vulnerability Note VU#878044 to these vulnerabilities.

  Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-0960 has been assigned to these vulnerabilities.

  This advisory will be posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20080610-snmpv3.shtml

Wide-Area Networking

- CSCse70647

  Symptoms: A router that functions as a BRAS or LNS crashes and generates one of the following error messages (or an error message that is similar to one of the following error messages):

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10, PC = 0x607C0374
  ```

  or

  ```
  %SYS-2-CHUNKFREE: Attempted to free nonchunk memory, chunk 206BCF18, data 21CD607D.
  -Process= "PPPoA Manager", ipl= 0, pid= 220
  ```

or

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

Conditions: This symptom is observed during PPP negotiations with a Microsoft PPP client that requests WINS or DNS data. Note that the symptom does not occur on a router that functions as a LAC.

Workaround: There is no workaround. However, entering the **ppp max-failure 100** command may reduce the chances that the symptom occurs.

- CSCse96387

  Symptoms: In a large scale Broadband Access Aggregation (BBA) environment, PPP negotiation may become stuck in a state in which one side is closed and the other side is constantly attempting to request options. This situation may cause all sessions to become stuck in a bad state that you must manually clear in order to recover from the state.

  Conditions: This symptom is observed on a Cisco router when a large volume of sessions comes up all at once as is common in an PPPoA BBA environment.

  Workaround: If you think you are encountering this caveat, please contact Cisco Technical Support Services for assistance and possible configuration tuning to minimize the chance that the symptom occurs again.

  Further Problem Description: If this is an option for your configuration, you can also reduce the rate of the incoming sessions to minimize the chance that the symptom occurs again.

- CSCsf06190

  Symptoms: Some PPP sessions do not properly synchronize to the standby RP.

  Conditions: This symptom is observed on a Cisco router that is configured for HA when many PPP interfaces flap at the same time.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(28)SB3

Cisco IOS Release 12.2(28)SB3 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(28)SB3 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 contains the fix for caveat CSCeh31423. See the information in the Bug Toolkit:

  http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCeh31423

  Workaround: There is no workaround.

IP Routing Protocols

- CSCeh83666

  Symptoms: A router may crash or fail to allocate a port.

Conditions: This symptom is observed on a Cisco router that is configured for NAT Overload and occurs because the “prev_block” pointer may be dereferenced when it is NULL.

Workaround: There is no workaround.

Miscellaneous

- CSCsb72921

  Symptoms: A QoS policy map that includes the **priority** and **police** commands in the same class may be rejected.

  Conditions: This symptom is observed on a Cisco router when you migrate from Cisco IOS Release 12.2S to either Release 12.2SB or Release 12.2SBC.

  Workaround: Edit the policy manually; enter the **police** command before you enter the **priority** command, and save the configuration.

  Further Problem Description: The symptom occurs because the bandwidth allocations are checked while the policy is being configured. In earlier Cisco IOS releases such as Release 12.2(25)S, the bandwidth allocations are checked only when the complete policy is attached to the interface. Because the **police** command provides the bandwidth limit for the **priority** command in this configuration, you must enter the **police** command before you enter the **priority** command.

- CSCsd44856

  Symptoms: A Cisco 10000 series crashes when you unconfigure MLP.

  Conditions: This symptom is observed when you first remove the controller and then remove a member of a bundle that belongs to the controller.

  Workaround: First remove all the bundles from the controller before you remove the controller.

- CSCsd80857

  Symptoms: An LFIB entry in the PXF engine may become corrupted, preventing from forwarding traffic.

  Conditions: This symptom is observed on a Cisco 10000 series when first a VRF is removed and then a link flap occurs.

  Workaround: Clear the affected route.

- CSCse25130

  Symptoms: IPCP renegotiations of an MLP interface may time out during renegotiation after an MR-APS failure has occurred.

  Conditions: This symptom is observed on a Cisco 10000 series that functions in an MR-APS configuration with another Cisco 10000 series.

  Workaround: There is no workaround.

- CSCse39760

  Symptoms: A PA-CC does not recover when you perform a soft or hard OIR of the standby RP.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with dual RPs after a switchover has occurred that causes the standby RP to become the active RP. In this situation, when you perform a soft or hard OIR of the standby RP, the PA-CC does not recover because the PA-CC fails to initialize.

  Workaround: There is no workaround.

- CSCse47922

  Symptoms: WRED random drops that occur in different ToS and DSCP classes do not correlate with the configured thresholds as you would expect.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100.

  Workaround: There is no workaround.

- CSCse61834

  Symptoms: When you modify an ATM PVC by entering the **pvc** *vpi/vci* command, any subsequent modifications in the VC class that is assigned to this PVC do not take effect.

  Conditions: This symptom is observed when the PVC is preconfigured with a VC class when the following events occur:

  1. You make a configuration change in the PVC.
  2. You change the configuration in the VC class.

  The configuration change in the VC class does not take effect.

  Workaround: First complete the configuration changes in the VC class. Then, change the configuration in the PVC.

Resolved Caveats—Cisco IOS Release 12.2(28)SB2

Cisco IOS Release 12.2(28)SB2 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(28)SB2 but may be open in previous Cisco IOS releases.

Basic System Services

- CSCeg63395

  Symptoms: A large latency may occur when packets are forwarded by a router.

  Conditions: This symptom is observed on a Cisco router when a DoS attack is launched from another router towards a POS interface of the Cisco router.

  Workaround: There is no workaround. Although the symptom causes performance degradation, it does not cause loss of functionality.

- 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.

- CSCsc64976

  A vulnerability exists in the IOS HTTP server in which HTML code inserted into dynamically generated output, such as the output from a show buffers command, will be passed to the browser requesting the page. This HTML code could be interpreted by the client browser and potentially execute malicious commands against the device or other possible cross-site scripting attacks. Successful exploitation of this vulnerability requires that a user browse a page containing dynamic content in which HTML commands have been injected.

Cisco will be making free software available to address this vulnerability for affected customers. 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-20051201-http.shtml

- CSCsd27777

  Symptoms: When you enter the **clear subscriber session all** command while traffic is being processed, the CPU usage of the router increases to 99 percent and sessions go down gradually. At the same time, the router automatically reinitiates sessions, and "%SSSMGR-3-MEMORY_LOW" and "%IDMGR-3-INVALID_ID:" error messages are generated. Eventually, the router generates "%TCP-6-NOBUFF:" and "%SYS-2-MALLOCFAIL" errors messages, and either resets all its interfaces or reloads.

  Conditions: This symptom is observed on a Cisco 10000 series that runs 16,000 PTA sessions with ISG features and 16,000 plain L2TP sessions. On all sessions, stateless traffic is being processed. The symptom is not specific to a Cisco 10000 series and may occur on other platforms that function in a similar configuration.

  Workaround: Do not clear all sessions at once via the **clear subscriber session all** command.

- CSCse11615

  Symptoms: When you enter the **enable** privileged EXEC command, an "Access Denied" message is generated.

  Conditions: This symptom is observed on a Cisco router when you have configured AAA authentication and when the **enable password** global configuration command is configured.

  Workaround: Configure the password for the **enable password** global configuration command to be no more than two characters.

  Alternate Workaround: Remove the **enable password** global configuration command from the startup configuration.

Miscellaneous

- CSCef82084

  Symptoms: Spurious memory accesses occur on a Cisco 7200 series and ALIGN-3-SPURIOUS error messages are generated.

  Conditions: This symptom is observed on a Cisco 7200 series that processes traffic through a serial interface.

  Workaround: There is no workaround.

- CSCeh40183

  Symptoms: A router reloads unexpectedly when the **show policy interface** EXEC command is entered.

  Conditions: This symptom is observed on a Cisco router when two users are connected to the router and simultaneously enter the **show policy interface** EXEC command.

  Workaround: Ensure that only one user at a time enters the command.

- CSCei27448

  Symptoms: A router may crash while displaying the output of the **show ip pim mdt bgp** command.

  Conditions: This symptom is observed when withdraws for a MDT source group are received by PIM from BGP while you enter the **show ip pim mdt bgp** command.

Workaround: There is no workaround. To reduce the chance of the router crashing, change the *screen-length* argument in the **terminal length** *screen-length* command to 0. Doing so prevents the router from pausing between multiple output screens. (The default of the *screen-length* argument is 24.)

- 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.

- CSCek20952

  Symptoms: The following error message may be generated when you configure a police statement in a policy map:

  ```
  Maximum rate for the policer is 0, conform action is drop
  ```

  Conditions: This symptom is observed on a Cisco router that functions in a L2VPN configuration with QoS features.

  Workaround: There is no workaround.

- CSCek25822

  Symptoms: A PRE crashes when you enter the **set cos** command for a HQoS parent policy map that is applied to an egress interface.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs whether or not the router processes traffic.

  Workaround: Do not enter the **set cos** command for a HQoS parent policy map that is applied to an egress interface.

  Further Documentation: The above-mentioned configuration is not supported on the Cisco 10000 series.

- CSCek30152

  Symptoms: When a T3/E3 Serial SPA is configured in Kentrox mode with a small bandwidth between 22 kbps and 250 kbps, either in T3 or E3 mode, the firmware miscalculates the bandwidth allocation and allows up to 24M of traffic to pass through.

  Conditions: This symptom is observed on a Cisco 7304 and a Cisco 12000 series.

  Workaround: Do not configure such a small bandwidth when the T3/E3 Serial SPA is configured in Kentrox mode. The minimal bandwidth on a T3/E3 Serial SPA that is configured in Kentrox mode is either 1500 kbps in T3 mode or 1000 kbps in E3 mode.

- CSCek35146

  Symptoms: When you remove and re-insert an MSC-100 card in which one or two SPAs are installed, the SPAs may become disabled for 10 to 12 minutes, after which they recover automatically.

  Conditions: This symptom is observed on a Cisco 7304 when you perform either a physical OIR or a soft-OIR by entering the **hw-module slot** *slot-number* **stop** command followed by the **hw-module slot** *slot-number* **start** command. The symptom occurs only when the time between the removal and the re-insertion is 2 to 3 seconds.

  Workaround: Do not re-insert the MSC-100 card too quickly after you have removed it. Wait at least 10 seconds before you re-insert the card.

- CSCek37011

  Symptoms: A line card may crash when you attempt to remove the child policy from the HQoS parent.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router when the line card has an interface that is configured as follows:

  - The interface faces the MPLS core.
  - The interface has an HQoS policy with a child policy.
  - The HQoS policy has a classification that is based on the MPLS EXP bits.

  Workaround: There is no workaround.

- CSCek39877

  Symptoms: A 4-port OC-3 ATM line card may not perform an APS switchover when a signal degrade (SD) or signal fail (SF) condition is present.

  Conditions: This symptom is observed on a Cisco 10000 series when bit errors occur on the on the 4-port OC-3 ATM line card.

  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.

- CSCin96524

  Symptoms: Control plane traffic may be dropped from a multilink interface.

  Conditions: This symptom is observed only when the multilink interface is oversubscribed and does not occur under normal traffic conditions.

  Workaround: Reduce the traffic rate.

  Alternate Workaround: Apply some type of queueing mechanism on the interface.

- CSCin97726

  Symptoms: On a Cisco 7500 router, the console of the active RSP may hang.

  Conditions: This symptom is observed when the router functions in RPR mode and when you attempt to access the standby RSP file system from the console of the active RSP, for example, by entering the **write memory** command or the **dir slavedisk0:** command.

  Note that the symptom is not specific to the Cisco 7500 series and may also occur on other platforms.

  Workaround: There is no workaround.

  Further Problem Description: Normal operation of the router is not affected, but the console becomes inaccessible.

- CSCsb01043

  Symptoms: When a Turbo ACL classification table grows beyond a certain size, a memory allocation failure may occur or the router may crash.

  If the router runs Cisco IOS Release 12.1E or 12.3, memory corruption may occur, causing the router to crash. If the router runs Cisco IOS Release 12.2S, an error message similar to the following may appear during a Turbo ACL compilation, the compilation will fail, and a recompilation is forced:

  ```
  %SYS-2-CHUNKBADELESIZE: Chunk element size is more than 64k for TACL Block -Process=
  "TurboACL", ipl= 0, pid= 82
  ```

  These symptoms do not occur because of an out-of-memory condition.

  Conditions: This symptom is observed on a Cisco router that is configured for Turbo ACL. The Cisco 10000 series is not affected.

  Workaround: Monitor the output of the **show access-lists compiled** command and force the Turbo ACL tables to be cleared if a table is at risk of growing large enough to trigger the symptoms.

  The tables that have significant sizes are the first and third tables shown next to “L1:” and the first table shown next to “L2:”. When the number after the slash for one of these tables is greater than 16384 for the “L1” tables or greater than 32768 for the “L2” table, the table is already too large and the symptom may occur any moment.

  When the number is in the range from 10924 to 16384 inclusive for the “L1” tables or the range from 21846 to 32768 inclusive for the “L2” tables, the table size will be too large on the next expansion. An expansion occurs when the number to the left of the slash reaches 90 percent of the value to the right of the slash. When the value to the left of the slash approaches 90 percent of the value to the right, enter the **no access-list compiled** command followed by the **access-list compiled** command to disable and re-enable Turbo ACL. Doing so causes the tables to be cleared and, therefore, delay the expansion. This workaround may be impractical when there is a high rate of incoming packets and when entries are added frequently to the tables.

  Alternative Workaround: Disable Turbo ACL by entering the **no access-list compiled** command.

  Note that neither of these workarounds are supported on a Cisco 7304 that is configured with an NSE-100: there is no workaround for this platform.

- CSCsb13836

  Symptoms: A Cisco 7304 may crash because of a bus error during normal operation when a external flash card is present.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 and that runs Cisco IOS Release 12.2(20)S4 or Release 12.2(20)S8. The symptom may also occur in other releases.

  Workaround: Do not use an external flash card. Rather, use an internal flash card.

- CSCsb33258

  Symptoms: An RP crashes during BGP convergence when MVPNs are configured.

  Conditions: This symptom is observed on a Cisco router after a duplicate BGP MDT extended community message is received that specifies a different Route Descriptor (RD) for an MDT that already exists for the specified MDT source and group address.

  Workaround: There is no workaround.

- CSCsb64858

  Symptoms: A switch or router may crash while processing a longest match lookup in the CEF table.

Conditions: This symptom is observed on a Cisco platform when a packet is punted because of an exception such as the occurrence of an ICMP redirect message while a longest match lookup is performed in the CEF table.

Workaround: Disable ICMP redirect messages by entering the **no ip redirects** interface configuration command on all interfaces of the router.

- CSCsb83990

  Symptoms: All on-demand VCs may become stuck in the inactive state because of insufficient bandwidth on one ATM interface.

  Conditions: This symptom is observed on a Cisco 10000 series when the creation of a VC fails because there are no more VCCIs, a line card failure occurs, or a toaster failure occurs. Each of these situations cause the ATM bandwidth to be depleted, and, in turn, prevent bandwidth from being available for any other ATM subinterfaces.

  Workaround: There is no workaround.

- CSCsc08491

  Symptoms: A virtual-access subinterface may not forward any traffic.

  Conditions: This symptom is observed on a Cisco router with a virtual-access application that causes virtual-access subinterface to be created.

  Workaround: There is no workaround.

- CSCsc37472

  Symptoms: The output rate counters for a member link of a multilink interface do not increment when you look at the output of the **show interfaces** command.

  Conditions: This symptom is observed on a Cisco 10000 series when packets are properly delivered through the member link of the multilink interface.

  Workaround: Look at the PXF counters in the output of the **show pxf cpu queue multilink** *interface* or **show pxf cpu subblock multilink** *interface* commands.

- 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.

- CSCsc78707

  Symptoms: The **mpls l2transport route** command may be rejected as an invalid input.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(27)SBC or Release 12.2(28)SB.

Workaround: There is no workaround.

- CSCsc86262

  Symptoms: When you configure OAM on an ATM subinterface in an AToM configuration, the ATM subinterface goes down.

  Conditions: This symptom is observed on a Cisco 7304 that has a NSE-100 and that functions as a PE router in an MPLS backbone.

  Workaround: There is no workaround. Note that the symptom does not occur when you disable the PXF engine.

- CSCsc90843

  Symptoms: A router that is configured with a multilink bundle may reload unexpectedly with the following error message:

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

  Conditions: This symptom is observed on a Cisco router when you attempt to remove a service policy from a multilink interface.

  Workaround: There is no workaround.

- CSCsd00354

  Symptoms: The output of the **show policy-map interface** command shows the output queue packets and bytes counters as zero.

  Conditions: This symptom is observed on a Cisco 10000 series on queues for which a policer is applied.

  Workaround: Use the policer’s counters in the output of the **show policy-map interface** command to determine the number of forwarded and dropped packets and bytes for the queue.

- CSCsd14277

  Symptoms: A ping does not pass through a Fast Ethernet interface that functions in AToM port mode.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 and that has the **xconnect** interface configuration command enabled on the interface of a 1-port Fast Ethernet port adapter (PA-FE) that is installed in a port adapter carrier card (7300-CC-PA).

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

  Alternate Workaround: Enter the **shutdown** interface configuration command, the **xconnect** interface configuration command, and then the **no shutdown** interface configuration command on the affected interface.

- CSCsd25699

  Symptoms: MLP traffic fails during a PRE failover of the protect router.

  Conditions: This symptom is observed on a Cisco 10000 series when a PRE failover occurs on the protect router because of an MR-APS cable break failover from the protect router to the working router.

  Workaround: If the active controller is brought up after the MR-APS failover, manually reverse APS.

- CSCsd35958

  Symptoms: A Cisco 7304 that is configured with an NPE-G100 processor and ATM VCs may reload unexpectedly.

  Conditions: This symptom is observed when a hierarchical policy on an ATM VC has the **shape average** command enabled.

  Workaround: Do not use a hierarchical policy on an ATM VC.

- CSCsd44475

  Symptoms: A ping may fail when packets pass from an MPLS VPN into a GRE tunnel.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100, that functions as a PE router, and that is connect to the MPLS core via a serial interface.

  Possible Workaround: Do not use a serial interface to connect the PE router to the MPLS core. Rather, use another type of interface.

  Further Problem Description: The symptom occurs because the tunnel adjacency is not complete in the PXF engine, preventing packets from being correctly punted and the adjacency from becoming complete.

- CSCsd49072

  Symptoms: The output of the **show policy-map interface** command shows incorrect statistics for a DSCP-based WRED policy. Also, when the class-map parameters are dynamically changed, the WRED statistics are lost.

  Conditions: These symptoms are observed on a Cisco 7304 that has an NSE-100.

  Workaround: There is no workaround.

- CSCsd49196

  Symptoms: After you have configured ingress NetFlow on an interface, the output of the **show ip cache verbose flow** command may show incorrect values in the “Active” seconds column.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S9, Release 12.2(20)S10, or Release 12.2(25)S8 when the **ip flow ingress** command is configured on an interface. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCsd58203

  Symptoms: The output of the **show ip cache flow** command, may shows some flows with a size of 4294M, which is the maximum size that can fit in a 32-bit value (2^32). Note that you can view the flows more easily in the output of the **show ip cache flow | i M|Pkts** command.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(25)S7. The symptom may occur in other releases.

  Workaround: There is no workaround.

  Further Problem Description: The symptom is of a cosmetic nature. Proper operation of the router is not affected.

- CSCsd62942

  Symptoms: The PXF engine on a Cisco 7304 that functions as a PE router may crash when traffic passes from the MPLS core to a CE router.

  Conditions: This symptom is observed when the traffic from the MPLS core is de-aggregated on the PE router into CE-facing interfaces that are configured into a VRF and that perform IP load-sharing and occurs while the PXF engine is active on the PE router.

Workaround: Disable IP-load-sharing on any interfaces that are configured into a VRF, such as the CE-facing interfaces.

Alternate Workaround: Disable PXF packet-processing on the PE router.

- 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:

     a. 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

     b. 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*

c. Apply the service policy (“my-class-default”) to the dot1q subinterface.

- CSCsd68659

  Symptoms: When you change the **atm dsx3mode** command for the framing of one port of a 8-port E3/DS3 ATM line card (ESR-8E3/DS3-ATM), all ports on the line card are affected.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsd69402

  Symptoms: Pre-classification on a GRE tunnel does not function.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 processor.

  Workaround: There is no workaround.

- CSCsd71131

  Symptoms: A service policy may be suspended when you enter the **clear interface** command for a multilink interface that has six members.

  Conditions: This symptom is observed on a Cisco router that is configured for dLFIoLL and QoS.

  Workaround: There is no workaround.

- CSCsd76528

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

  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.

  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.

- CSCsd83503

  Symptoms: NetFlow updates only MPLS-related egress records but not IPv4 ingress records.

  Symptoms: This symptom is observed on a Cisco 10000 series that has an PRE-2 and that has the **ip route-cache flow** command enabled on its main ATM and GE interfaces and the **mpls netflow egress** command enabled on its ATM subinterfaces (on which PVCs are configured) and GE subinterfaces.

  Note that the **ip route-cache flow** command is automatically converted into the **ip flow ingress** command and the **mpls netflow egress** command is automatically converted into the **ip flow egress** command, and these commands are stored in NVRAM. The symptom occurs after you have reloaded the PRE-2.

Workaround: Disable and re-enable the **ip flow ingress** command on the main interfaces.

- CSCsd88288

  Symptoms: Packet loss may occur on a GRE tunnel on which CEF is enabled.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs the c7300-js-mz image of Cisco IOS Release 12.2(25)S8. The symptom may also occur in Release 12.2(27)SBC or Release 12.2(28)SB.

  Workaround: Disable PXF on the Cisco 7304. If this is not an option, there is no workaround.

- CSCsd91238

  Symptoms: The success rate of pings decreases when you increase the packet size of the pings, and the output of the **show ip traffic** command shows increasing ICMP checksum errors.

  Conditions: This symptom is observed on a Cisco 7304 that has a an NSE-100, that runs Cisco IOS Release 12.2(28)SB, and that is configured with a 2-port OC-3 ATM line card (7300-2OC3ATM-SMI) when MLP and VRF are enabled on a virtual template that automatically configures the ATM PVC bundle on the line card.

  Workaround: Disable VRF forwarding on the virtual template.

  Alternate Workaround: Disable PPP on the ATM PVC bundle.

- CSCsd93728

  Symptoms: A router that functions as an LNS may crash while processing traffic over L2TP connections, and the following error message is generated:

  ```
  Cause 00000010 (Code 0x4): Address Error (load or instruction fetch) exception
  ```

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(28)SB and that is configured for QoS. The symptom occurs during normal operation.

  Workaround: There is no workaround.

- CSCsd98928

  Symptoms: A router may crash when you enter the **show policy-map interface** command while an automated script completes the policy map and then removes the policy map during cleanup.

  Conditions: This symptom is observed on a Cisco router when you enter the **show policy-map interface** command while, at the same time, the automated script removes the policy map.

  Workaround: There is no workaround.

- CSCse00469

  Symptoms: When you boot the router, the SuperACL process causes a high CPU usage for an extended time, and not all configured policy maps are compiled.

  Conditions: This symptom is observed on a Cisco 10000 series when there are hundreds (or more) policy maps in the configuration.

  Workaround: Reduce the number of policy maps. If this is not an option, there is no workaround.

- CSCse00609

  Symptoms: Serial interfaces go down after an RP switchover.

  Conditions: This symptom is observed on a Cisco 10000 series that has serial interfaces configured on either a channelized OC-3 or channelized OC-12 line card.

  Workaround: There is no workaround to prevent the symptom from occurring. When the symptom has occurred. Bring the serial interfaces back up by resetting the line card.

- CSCse01030

  Symptoms: When an ATM interface has a QoS policy, locally generated traffic such as OSPF DPP traffic may not be transmitted.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(28)SB.

  Workaround: There is no workaround.

- CSCse06387

  Symptoms: A Cisco 7304 may reload unexpectedly after two HA switchovers have occurred.

  Conditions: This symptom is observed when 4000 virtual circuits are configured on the router.

  Workaround: There is no workaround.

- CSCse20029

  Symptoms: A router that is configured for MPLS and NetFlow may reload unexpectedly because of a bus error.

  Conditions: This symptom is observed on a Cisco router that has the **vpdn enable** and **ip vrf** commands enabled.

  Workaround: There is no workaround.

- CSCse51608

  Symptoms: When you enter the **xconnect** command, the command is not accepted.

  Conditions: This symptom is observed on a Cisco 7200 series, irrespective of which interface the command is entered for.

  Workaround: There is no workaround.

- CSCsd40334

  Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

  Cisco has made free software available to address this vulnerability for affected customers.

  There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

  This advisory is posted at
  http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml.

TCP/IP Host-Mode Services

- CSCek01499

  Symptoms: When a CE router that is configured for MPLS reloads, a software-forced crash may occur on the connected PE router because of memory corruption.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that has two RPs that function in SSO mode. The symptom does not occur when the router has only a single RP.

  Workaround: There is no workaround.

- CSCek37177

  The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

  This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

  Cisco has made free software available to address this vulnerability for affected customers.

  This issue is documented as Cisco bug ID CSCek37177.

  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-20070124-crafted-tcp.shtml.

Wide-Area Networking

- CSCeh58376

  Symptoms: A serial interface on a channelized port adapter may stop forwarding traffic through the router but traffic to and from the router over the interface may still go through. The Tx accumulator "value" counter in the output of the **show controllers cbus** Exec command does not exceed the value 2, as is shown in the following example:

  ```
  Router#sh controllers cbus | include Serial5/1/0.1/2/6/2:0
  Serial5/1/0.1/2/6/2:0, txq E8001B40, txacc E8000412 (value 2), txlimit 26
  ```

  Conditions: This symptom is observed on a Cisco 7500 series that runs Cisco IOS Release 12.0S when QoS is configured on at least one interface on the VIP in which the channelized port adapter is installed. The symptom occurs after the affected interface has flapped very frequently because of OSI layer 1 errors. The symptom may also occur in other releases.

  Workaround: Remove and reconfigure the controller of the affected interface.

- CSCek24091

  Symptoms: A PPP session fails to come up, and the following debug message is generated:

  ```
  PPP SSS: stale named authen method list "default"
  ```

  Conditions: This symptom is observed only when a service policy is applied and when the default PPP authentication method list is used.

  Workaround: Use a PPP authentication method list other than the PPP authentication default method list.

- CSCek32043

  Symptoms: cRTP may become disabled on an interface when you disable and re-enable the **ip rtp header-compression** command on the interface.

  Conditions: This symptom is observed on a Cisco router that functions in an MLP configuration when the link (such as a Frame Relay link) and the MLP bundle clone from the same virtual template.

  Workaround: Reset the interface.

- CSCsc28120

  Symptoms: A Cisco 7301 may crash when a service policy is removed from an interface that is configured for Frame Relay encapsulation.

Conditions: This symptom is observed when a service policy is configured on an interface before the encapsulation is changed to Frame Relay. When the service policy is then removed, the router crashes.

Workaround: Remove the service policy before you change the encapsulation to Frame Relay.

- CSCsd71360

  Symptoms: PPP Multilink fragment loss occurs as the result of premature lost fragment timeouts. This can be seen in the lost fragment count in the output of the **show ppp multilink** command, as well as debug traces produced by the **debug ppp multilink events** command.

  Conditions: This symptom has been observed with Cisco IOS Release 12.2(28)SB and Release 12.4(6)T, but not with Cisco IOS Release 12.2(27)SBC2 or Release 12.4(4)T.

  Workaround: Configure the **ppp timeout multilink lost-fragment 1** command under the Multilink interface or the Virtual-Template interface corresponding to the multilink bundle.

Resolved Caveats—Cisco IOS Release 12.2(28)SB1

Cisco IOS Release 12.2(28)SB1 is a rebuild release for Cisco IOS Release 12.2(28)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(28)SB1 but may be open in previous Cisco IOS releases. Cisco IOS Release 12.2(28)SB1 support the Cisco 7304 only.

IP Routing Protocols

- CSCek26492

  Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

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

  Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

  Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

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

Miscellaneous

- CSCek35146

  Symptoms: When you remove and re-insert an MSC-100 card in which one or two SPAs are installed, the SPAs may become disabled for 10 to 12 minutes, after which they recover automatically.

  Conditions: This symptom is observed on a Cisco 7304 when you perform either a physical OIR or a soft-OIR by entering the **hw-module slot** *slot-number* **stop** command followed by the **hw-module slot** *slot-number* **start** command. The symptom occurs only when the time between the removal and the re-insertion is 2 to 3 seconds.

  Workaround: Do not re-insert the MSC-100 card too quickly after you have removed it. Wait at least 10 seconds before you re-insert the card.

- CSCsb13836

  Symptoms: A Cisco 7304 may crash because of a bus error during normal operation when a external flash card is present.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 and that runs Cisco IOS Release 12.2(20)S4 or Release 12.2(20)S8. The symptom may also occur in other releases.

  Workaround: Do not use an external flash card. Rather, use an internal flash card.

- CSCsc86262

  Symptoms: When you configure OAM on an ATM subinterface in an AToM configuration, the ATM subinterface goes down.

  Conditions: This symptom is observed on a Cisco 7304 that has a NSE-100 and that functions as a PE router in an MPLS backbone.

  Workaround: There is no workaround. Note that the symptom does not occur when you disable the PXF engine.

- CSCsd44475

  Symptoms: A ping may fail when packets pass from an MPLS VPN into a GRE tunnel.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100, that functions as a PE router, and that is connect to the MPLS core via a serial interface.

  Possible Workaround: Do not use a serial interface to connect the PE router to the MPLS core. Rather, use another type of interface.

  Further Problem Description: The symptom occurs because the tunnel adjacency is not complete in the PXF engine, preventing packets from being correctly punted and the adjacency from becoming complete.

- CSCsd49072

  Symptoms: The output of the **show policy-map interface** command shows incorrect statistics for a DSCP-based WRED policy. Also, when the class-map parameters are dynamically changed, the WRED statistics are lost.

  Conditions: These symptoms are observed on a Cisco 7304 that has an NSE-100.

  Workaround: There is no workaround.

- CSCsd49196

  Symptoms: After you have configured ingress NetFlow on an interface, the output of the **show ip cache verbose flow** command may show incorrect values in the "Active" seconds column.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(20)S9, Release 12.2(20)S10, or Release 12.2(25)S8 when the **ip flow ingress** command is configured on an interface. The symptom may also occur in other releases.

  Workaround: There is no workaround.

- CSCsd58203

  Symptoms: The output of the **show ip cache flow** command, may shows some flows with a size of 4294M, which is the maximum size that can fit in a 32-bit value (2^32). Note that you can view the flows more easily in the output of the **show ip cache flow | i M|Pkts** command.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(25)S7. The symptom may occur in other releases.

  Workaround: There is no workaround.

Further Problem Description: The symptom is of a cosmetic nature. Proper operation of the router is not affected.

- CSCsd62942

  Symptoms: The PXF engine on a Cisco 7304 that functions as a PE router may crash when traffic passes from the MPLS core to a CE router.

  Conditions: This symptom is observed when the traffic from the MPLS core is de-aggregated on the PE router into CE-facing interfaces that are configured into a VRF and that perform IP load-sharing and occurs while the PXF engine is active on the PE router.

  Workaround: Disable IP-load-sharing on any interfaces that are configured into a VRF, such as the CE-facing interfaces.

  Alternate Workaround: Disable PXF packet-processing on the PE router.

- CSCsd69402

  Symptoms: Pre-classification on a GRE tunnel does not function.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 processor.

  Workaround: There is no workaround.

- CSCsd88288

  Symptoms: Packet loss may occur on a GRE tunnel on which CEF is enabled.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs the c7300-js-mz image of Cisco IOS Release 12.2(25)S8. The symptom may also occur in Release 12.2(27)SBC or Release 12.2(28)SB.

  Workaround: Disable PXF on the Cisco 7304. If this is not an option, there is no workaround.

- CSCsd91238

  Symptoms: The success rate of pings decreases when you increase the packet size of the pings, and the output of the **show ip traffic** command shows increasing ICMP checksum errors.

  Conditions: This symptom is observed on a Cisco 7304 that has a an NSE-100, that runs Cisco IOS Release 12.2(28)SB, and that is configured with a 2-port OC-3 ATM line card (7300-2OC3ATM-SMI) when MLP and VRF are enabled on a virtual template that automatically configures the ATM PVC bundle on the line card.

  Workaround: Disable VRF forwarding on the virtual template.

  Alternate Workaround: Disable PPP on the ATM PVC bundle.

- CSCse01030

  Symptoms: When an ATM interface has a QoS policy, locally generated traffic such as OSPF DPP traffic may not be transmitted.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100 and that runs Cisco IOS Release 12.2(28)SB.

  Workaround: There is no workaround.

- CSCse06387

  Symptoms: A Cisco 7304 may reload unexpectedly after two HA switchovers have occurred.

  Conditions: This symptom is observed when 4000 virtual circuits are configured on the router.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(28)SB

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(28)SB. All the caveats listed in this section are open in Cisco IOS Release 12.2(28)SB. This section describes only severity 1, severity 2, and select severity 3 caveats.

Basic System Services

- CSCsc17888

  Symptoms: FRoMPLS traffic does not pass through the first port of an 8-port multichannel T1/E1 8PRI (PA-MC-8TE1+).

  Conditions: This symptom is observed on a Cisco router that functions as a CE router in an AToM environment when the ports of the PA-MC-8TE1+ are configured for E1. Note that the symptom does not occur for IP traffic and L3 traffic on the first port of the PA-MC-8TE1+, nor for the remaining seven E1 ports.

  Workaround: There is no workaround.

- CSCsd27777

  Symptoms: When you enter the **clear subscriber session all** command while traffic is being processed, the CPU usage of the router increases to 99 percent and sessions go down gradually. At the same time, the router automatically reinitiates sessions, and "%SSSMGR-3-MEMORY_LOW" and "%IDMGR-3-INVALID_ID:" error messages are generated. Eventually, the router generates "%TCP-6-NOBUFF:" and "%SYS-2-MALLOCFAIL" errors messages, and either resets all its interfaces or reloads.

  Conditions: This symptom is observed on a Cisco 10000 series that runs 16,000 PTA sessions with ISG features and 16,000 plain L2TP sessions. On all sessions, stateless traffic is being processed. The symptom is not specific to a Cisco 10000 series and may occur on other platforms that function in a similar configuration.

  Workaround: Do not clear all sessions at once via the **clear subscriber session all** command.

- CSCsd38237

  Symptoms: The active RP or PRE may reload in the "db_record_set_field" function when the router runs out of memory resources.

  Conditions: This symptom is observed on a Cisco router that is configured with many sessions and occurs because the ID manager cannot not enqueue the "db_field" to the "db_record" when the router runs out of memory resources.

  Workaround: Limit the number of sessions on the router to ensure that there are sufficient memory resources.

IP Routing Protocols

- CSCeh91717

  Symptoms: When IPv4 routes are imported into a VRF, the routes in the VRF CEF table are marked as "unusable" and "no label".

  Conditions: This symptom is observed on a Cisco router when the "BGP Support for IP Prefix Import from a Global Table into a VRF Table" feature is enabled and when you enter the **import ipv4 unicast** command under a VRF.

  Workaround: There is no workaround.

- CSCej72829

  Symptoms: Some BGP SSO peers become disabled.

  Conditions: This symptom is observed after an SSO switchover occurs on a Cisco router.

  Workaround: There is no workaround. Note that after five minutes the BGP SSO peers are automatically re-enabled.

- CSCsc37461

  Symptoms: A PE router that functions in an MPLS VPN configuration may take a long time to converge.

  Conditions: This symptom is observed when an interface goes down and when an MP-BGP next hop that points to this interface is no longer reachable. This MP-BGP next hop remains unreachable until the Interior Gateway Protocol (IGP) finds an alternate path. If the BGP scanner runs while the MP-BGP next hop is unreachable, VRF routes that use this MP-BGP next hop may be removed from the VRF routing table. However, usually, when the next BGP scanner runs, these VRF routes are updated and then re-imported into VRF routing table.

  Workaround: The probability for the symptom to occur depends on the elapse time between the interface going down and the IGP convergence and can be decreases by tuning the IGP parameters for a faster convergence.

- CSCsd17747

  Symptoms: When you enter the **ip pim vrf register-source** command on an interface and then delete the interface or its IP address, the command remains in the configuration. This situation causes the bulk synchronization to fail and the standby RP to reset continuously after an RP switchover has occurred. Then, because the register source (the interface) cannot be found, a BEM failure occurs.

  Conditions: These symptoms are observed when the interface forwards traffic from a nondefault VRF and when the interface has a register source configured.

  Workaround: Remove the **ip pim vrf register-source** command from the interface before you delete the interface or its IP address.

Miscellaneous

- CSCef47220

  Symptoms: A path trace buffer value may be displayed as UNSTABLE in the output of the **show controllers** command when you enter this command for an AU-3 port and look for the overhead bytes.

  Conditions: This symptom is observed on a Cisco 10000 series that has a 4-port channelized OC-3 line card with an E1 interface that is configured for AU-3. The E1 interface has the **overhead j1 length 16 transmit-message** *string* command enabled.

  Workaround: There is no workaround.

- CSCef47280

  Symptoms: A T1 interface that is configured for AU-4 mapping on a 4-port channelized OC-3 line card does not come up.

  Conditions: This symptom is observed on a Cisco 10000 series when the T1 interface interoperates with a third-party vendor test analyzer device.

  Workaround: There is no workaround.

- CSCeg11769

  Symptoms: When class-based weighted fair queueing (CBWFQ) is configured, the router may not match the input packet rate.

  Conditions: This symptom is observed on a Cisco router that is configured for ATM and Frame Relay.

  Workaround: There is no workaround.

- CSCeg69418

  Symptoms: You cannot re-enable Home Agent (HA) functionality on a router after you have first unconfigured it.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SB and that is configured for mobile IP.

  Workaround: There is no workaround.

- CSCeg88253

  Symptoms: Loss of packets may occur on video queues.

  Conditions: This symptom is observed on a Cisco 10000 series that has Class-Based Weighted Fair Queueing (CBWFQ) configured on a PPP over Ethernet over ATM (PPPoEoA) link and occurs when traffic is being processed.

  Workaround: There is no workaround.

- CSCeh54607

  Symptoms: On a router that processes a high traffic rate, the output of the **show processes cpu** command shows 100 percent CPU usage.

  Conditions: This symptom is observed on a Cisco router when the following conditions are present:

  - The router processes 70 PTA PPPoE sessions.
  - There are 70,000 packets per second with 120 bytes per packet upstream.
  - There are 5600 packets per second with 1500 bytes per packet downstream.

  Workaround: Reduce the traffic rate.

- CSCei38741

  Symptoms: Tracebacks are generated on a Cisco 10000 series that is configured with serial interfaces.

  Conditions: This symptom is observed when you change the encapsulation on a serial interface from PPP to Frame Relay.

  Workaround: Before you change the encapsulation from PPP to Frame Relay, enter the **no encapsulation ppp** command.

- CSCei54002

  Symptoms: A QoS group that is set through QoS Policy Propagation via BGP (QPPB) may not function.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a PRE2.

  Workaround: Use QPPB to set the IP precedence.

- CSCej02774

  Symptoms: When you use the **BREAK** key to interrupt the image boot process and then enter the **dir** command from the ROMmon prompt, a recurring “Arithmetic Overflow Exception” may occur.

Conditions: This symptom is observed on a Cisco 10000 series that has 104480 Kbytes of main memory and occurs only when a file system device driver is recursively loaded because you used the **BREAK** key to interrupt the image boot process and then entered the **dir** command without first resetting the ROMmon.

Workaround: Let the image boot and then enter the **dir** command. If you must interact with the file system via the ROMmon when the boot process has been interrupted, enter the **reset** command. If autoboot is enabled, use the **BREAK** key immediately after the banner line appears on screen.

- CSCej46675

  Symptoms: A ping over an MLP connection may fail.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with 336 bundles with 3 links each. Note that the symptom does not occur when the router has 100 bundles with 10 links each or 126 bundles with 8 links each.

  Workaround: There is no workaround.

- CSCej63166

  Symptoms: A router that is configured as an LSR may generate a "%LSD-4- LABEL_RESOURCE" error message when you attempt to extend the label range.

  Conditions This symptom is observed when the LSR is configured with a limited label range when you attempt to extend the label range.

  Workaround: Enter the **no mpls label range** command and reconfigure the extended label range.

- CSCej87817

  Symptoms: Policing does not drop any packets after the packets are sent or received at a rate that is much higher than the committed information rate (CIR).

  Conditions: This symptom is observed on a Cisco 7500 series router but is not platform dependent.

  Workaround: There is no workaround.

- CSCek00986

  Symptoms: A configuration does not synchronize to the standby RP and a traceback is generated.

  Conditions: This symptom is observed on a Cisco router that has dual RPs and that has the **crypto key zeroize rsa** command enabled.

  Workaround: There is no workaround.

- 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.

- CSCek11664

  Symptoms: A forwarded packet may be lost on a PPPoE session.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCek21091

  Symptoms: PPPoX multicast traffic is process-switched by default. This is improper behavior.

Conditions: This symptom is observed when the **no ip mroute-cache** command is enabled for virtual-template interfaces, causing IP multicast traffic to be process-switched.

Workaround: Enter the **ip mroute-cache** command for each virtual-template interface.

- CSCek25123

  Symptoms: When you apply a HQoS policy that has a shape parameter of 1 Gb in its parent policy to a subinterface, a traceback is generated. When there are more than 112 subinterfaces, you cannot apply the policy map to interfaces that exceed the 112th subinterface.

  Conditions: This symptom is observed on a Cisco 10000 series when you apply or remove a HQoS policy to or from a subinterface and when the bandwidth in the parent policy map is 1 Gb.

  Workaround: There is no workaround.

- CSCek25822

  Symptoms: A PRE crashes when you enter the **set cos** command for a HQoS parent policy map that is applied to an egress interface.

  Conditions: This symptom is observed on a Cisco 10000 series and occurs whether or not the router processes traffic.

  Workaround: Do not enter the **set cos** command for a HQoS parent policy map that is applied to an egress interface.

  Further Documentation: The above-mentioned configuration is not supported on the Cisco 10000 series.

- CSCek27708

  Symptoms: A 1-port channelized OC-12 or 4-port channelized OC-3 line card may reset.

  Conditions: This symptom is observed on a Cisco 10000 series when you run a script that configures the line card with 768 E1 or T1 interfaces with either SDH or SONET framing.

  Workaround: There is no workaround.

- CSCek31331

  Symptoms: Gigabit Ethernet line cards flap and go down.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with multiple pairs of Gigabit Ethernet line cards when traffic flows at or is approaching the line rate.

  Workaround: Either turn on or turn off negotiation on the affected pair of line cards and the point of traffic generation.

- CSCek34834

  Symptoms: Input drops or packet drops may occur when a 1-port Gigabit Ethernet half-height line card is processing IMIX traffic.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with a 1-port Gigabit Ethernet half-height line card.

  Workaround: There is no workaround.

- CSCek36080

  Symptoms: A Cisco router that functions as an Intelligent Services Gateway (ISG) may reload when an error condition occurs in the control plane.

  Conditions: This symptom is observed under a rare conditions when an error occurs while a session that contains auto services is brought up or while a service profile that contains auto services is activated. The symptom occurs because of a timing issue.

Workaround: Do not use auto services in the user profile.

- CSCek56991

  Symptoms: A Cisco 7200 series may send a corrupted packet via a 2-port T3 serial, enhanced port adapter (PA-2T3+). The rate of corrupted packets is very low.

  Conditions: This symptom is observed on a Cisco 7200 series that runs Cisco IOS Release 12.2SB, Release 12.4T, or Release 12.4(4)XD3 and occurs when the router functions under high stress conditions such as a high CPU load and an oversubscribed interface of the PA-2T3+.

  Workaround: Avoid a high CPU load and oversubscription of the interface of the PA-2T3+.

- CSCin97726

  Symptoms: On a Cisco 7500 router, the console of the active RSP may hang.

  Conditions: This symptom is observed when the router functions in RPR mode and when you attempt to access the standby RSP file system from the console of the active RSP, for example, by entering the **write memory** command or the **dir slavedisk0:** command.

  Note that the symptom is not specific to the Cisco 7500 series and may also occur on other platforms.

  Workaround: There is no workaround.

  Further Problem Description: Normal operation of the router is not affected, but the console becomes inaccessible.

- CSCsa56416

  Symptoms: In order for Ethernet over MPLS (EoMPLS) to function properly in either port mode or VLAN mode, the Ethernet controller must operate in promiscuous mode, that is, all MAC address filtering must be disabled. On the 8-port Fast Ethernet (FE) line card, there is one single register that controls the enabling and disabling of address filtering for the whole line card. Therefore, if even one single EoMPLS circuit is created on any of the eight ports of the line card, address filtering is disabled for all eight ports, that is all eight ports operate promiscuous mode. This situation is not desirable.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for EoMPLS when you create an AToM circuit by entering the **xconnect** command on an Ethernet controller of the 8-port FE line card. In this situation, promiscuous mode is automatically enabled on the Ethernet controller and remains enabled for all eight ports of the line card until the last AToM circuit is removed from the Ethernet controller by entering the **no xconnect** command.

  Workaround: There is no workaround.

- CSCsb10347

  Symptoms: Multilink interfaces remain down after an SSO switchover.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for LFIoFR and occurs only when traffic is flowing while an SSO switchover occurs. When there is no traffic, the interfaces come up normally.

  Workaround: There is no workaround.

- CSCsb32888

  Symptoms: Forcing **release** or **renew** commands on a BVI interface fails.

  Conditions: The symptom has been observed on the Cisco 7200 platform.

  Workaround: There is no workaround.

- CSCsb36094

  Symptoms: Policing in the outward direction is not performed for IP packets with an “IP Options” payload.

  Conditions: This symptom is observed on a Cisco 10000 series that processes incoming IP packets with the “IP Options” field. The policing actions are ignored for the outgoing IP packet.

  Workaround: There is no workaround.

- CSCsb79060

  Symptoms: A T1 interface that is configured on a channelized OC-3 line card or OC-12 line card may send a Loss of Framing (LoF) alarm, causing the T1 interface to enter the down/down state. Even after you have entered the **loopback local** command, have configured HDLC encapsulation, and have configured the clock source as internal, the T1 interface does not transition to the up state.

  Another symptom is that the framing may be good, but the TX data path is not good, causing the T1 interface to enter the up/down state. The output counters on the PRE increment, but the packets never actually leave the channelized line card.

  Conditions: These symptoms are observed on a Cisco 10000 series.

  Workaround: Reload the channelized line card by entering the **hw-module slot** *slot-number* **reset** command.

- CSCsb97334

  Symptoms: After you reload the router, a glean adjacency is not resolved if the prefix is a tunnel destination.

  Conditions: This symptom is observed on a Cisco 7304 that has a tunnel configured when the destination is another tunnel.

  Workaround: Ping the tunnel interface of the destination to resolve the adjacency.

- CSCsc18999

  Symptoms: When you enter the **clear subscriber sessions all** command, the router reloads.

  Conditions: This symptom is observed when Transparent Autologon (TAL) is used with ISG for control over DHCP addressing and when the router is using nearly all available CPU cycles and RAM.

  Workaround: Do not you enter the **clear subscriber sessions all** command.

- CSCsc27712

  Symptoms: An ATM Permanent Virtual Path (PVP) goes down after a couple of minutes of non-activity.

  Conditions: This symptom is observed on a Cisco router when you enter the **atm pvp** command and leave the connection idle for a couple of minutes.

  Workaround: There is no workaround.

- CSCsc37472

  Symptoms: The output rate counters for a member link of a multilink interface do not increment when you look at the output of the **show interfaces** command.

  Conditions: This symptom is observed on a Cisco 10000 series when packets are properly delivered through the member link of the multilink interface.

  Workaround: Look at the PXF counters in the output of the **show pxf cpu queue multilink** *interface* or **show pxf cpu subblock multilink** *interface* commands.

- CSCsc48372

  Symptoms: The police function stops working when a PQ class map is removed and redefined for a policy map and when any class that is defined above the PQ class map is deleted. In this situation, all packets that match the PQ classes are marked as violated packets.

  Conditions: This symptom is observed on a Cisco 10000 series.

  Workaround: Remove the service policy and re-apply the service policy to the affected interfaces.

- CSCsc58937

  Symptoms: When you run the CISCO-FLASH-MIB, various traps are missing even though the operation is reported as successfully completed.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for SNMP.

  Workaround: There is no workaround.

- CSCsc60444

  Symptoms: A "PXF DMA Toaster Stall Error" may occur, the microcode may unexpectedly be reloaded onto the PXF engine, and the reusable bandwidth may be incorrectly shaped.

  Conditions: These symptoms are observed on a Cisco 10000 series when a hierarchical policy map is attached to a Gigabit Ethernet interface and when the hierarchical policy map has a shaped rate that exceeds the link rate.

  Workaround: Do not attach a policy map that has a shaped rate that exceeds the link rate.

- CSCsc71353

  Symptoms: The **xconnect** command is not accepted.

  Conditions: This symptom is observed on a Cisco 7304 when you attempt to configure the **xconnect** command on an IMA port adapter that is configured for AAL0 encapsulation.

  Workaround: There is no workaround.

- CSCsc84834

  Symptoms: An adjacency is not established when a GRE tunnel is configured.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100.

  Workaround: Ping the next hop through the GRE tunnel.

- CSCsc97102

  Symptoms: When you create or delete an PPPoX session, the address conversion from the RP to the eXternal Column Memory (XCM) is incorrect, as is shown by a traceback that is displayed on the console of the standby PRE.

  Conditions: This symptom is observed randomly on a Cisco 10000 series.

  Workaround: There is no workaround.

- CSCsd00354

  Symptoms: The output of the **show policy-map interface** command shows the output queue packets and bytes counters as zero.

  Conditions: This symptom is observed on a Cisco 10000 series on queues for which a policer is applied.

  Workaround: Use the policer's counters in the output of the **show policy-map interface** command to determine the number of forwarded and dropped packets and bytes for the queue.

- CSCsd08662

  Symptoms: A Cisco 7200 series may crash when you apply a service policy with a priority action on a control plane.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with an NPE-G1.

  Workaround: There is no workaround.

  Further Problem Description: A service policy with a priority action is not supported on a control plane. See the following Cisco document:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide0 9186a008052446b.html

- CSCsd14277

  Symptoms: A ping does not pass through a Fast Ethernet interface that functions in AToM port mode.

  Conditions: This symptom is observed on a Cisco 7304 that is configured with an NSE-100 and that has the **xconnect** interface configuration command enabled on the interface of a 1-port Fast Ethernet port adapter (PA-FE) that is installed in a port adapter carrier card (7300-CC-PA).

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

  Alternate Workaround: Enter the **shutdown** interface configuration command, the **xconnect** interface configuration command, and then the **no shutdown** interface configuration command on the affected interface.

- CSCsd25699

  Symptoms: MLP traffic fails during a PRE failover of the protect router.

  Conditions: This symptom is observed on a Cisco 10000 series when a PRE failover occurs on the protect router because of an MR-APS cable break failover from the protect router to the working router.

  Workaround: If the active controller is brought up after the MR-APS failover, manually reverse APS.

- CSCsd25713

  Symptoms: A Cisco 7304 crashes because of an address error (load or instruction fetch) exception when you remove a virtual template that is applied to at least one ATM subinterface by entering the **no interface virtual-template** command.

  Conditions: This symptom is observed on a Cisco 7304 that runs Cisco IOS Release 12.2(27)SBC1 and may also occur in Release 12.2(28)SB.

  Workaround: Dot no apply a virtual template to an ATM interface.

- CSCsd38522

  Symptoms: Very high CPU usage may occur on a Cisco 10000 series when several thousand PPPoX PTA sessions are established and when the Port-Bundle Host Key (PBHK) feature is enabled. This situation can be observed in the output of the **show processes cpu** command.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured as an Intelligent Service Gateway (ISG) and that has the PBHK feature enabled with the default traffic class.

  Workaround: Apply an explicit traffic class to the port bundle, that is, apply an IP ACL that has the IP address of the Subscriber Edge Services Manager (SESM) as its destination IP address. Doing so reduces the CPU usage considerably.

- CSCsd39557

  Symptoms: Non-priority traffic is dropped, and priority traffic is sent at a very low rate.

  Conditions: This symptom is observed on a Cisco 7304 that has an NPE-G100 when hierarchical shaping is configured on an ATM VC with a priority class in the next layer, as in the following example:

  policy-map *atm-pri600* **class** *From2_0* **priority** *150*

  policy-map *hiershape* **class** *class-default* **shape average** *1000000* **service-policy** *atm-pri600*

  interface *ATM4/0.401 point-to-point* **pvc** *1/401* **vbr-nrt** *600 600* **service-policy out** *hiershape*

  Workaround: There is no workaround to prevent the symptom from occurring. You can restore the flow by first removing the policy from the interface and then by entering the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the affected interface.

- CSCsd41107

  Symptoms: A Cisco 10000 series that functions as an LNS with a highly scaled configuration may reload unexpectedly.

  Conditions: This symptom is observed when the router runs very low on available processor memory. When this situation occurs, the following error messages are generated:

  ```
  GENERAL-2-CRITEVENT: Unable to malloc current_if_info C10K_BBA_SESSION-3-ERREVENT: No
  VCCI found for LNS session (26831)
  ```

  Workaround: Reduce or limit the number of L2TP tunnels and/or the number of PPP sessions that are being terminated on the LNS.

- CSCsd44475

  Symptoms: A ping may fail when packets pass from an MPLS VPN into a GRE tunnel.

  Conditions: This symptom is observed on a Cisco 7304 that has an NSE-100, that functions as a PE router, and that is connect to the MPLS core via a serial interface.

  Possible Workaround: Do not use a serial interface to connect the PE router to the MPLS core. Rather, use another type of interface.

  Further Problem Description: The symptom occurs because the tunnel adjacency is not complete in the PXF engine, preventing packets from being correctly punted and the adjacency from becoming complete.

- CSCsd49072

  Symptoms: The output of the **show policy-map interface** command shows incorrect statistics for a DSCP-based WRED policy. Also, when the class-map parameters are dynamically changed, the WRED statistics are lost.

  Conditions: These symptoms are observed on a Cisco 7304 that has an NSE-100.

  Workaround: There is no workaround.

- CSCsd51700

  Symptoms: A serial interface that is connected to an OSPP neighbor may flap during an SSO switchover, causing OSPF NSF to terminate during the switchover.

  Conditions: This symptom is observed on a Cisco 7304 that is configured for NSF and occurs after multiple (10 or more) SSO switchovers.

  Workaround: There is no workaround.

- CSCsd52476

  Symptoms: Some members of a multilink interface may flap when you enter the **write memory** command on the PRE. Flapping occurs randomly each time the router reloads.

  Conditions: There symptoms are observed on a Cisco 10000 series that is configured for SSO, MR-APS, and MLP with Link Fragmentation Interleave (LFI).

  Workaround: There is no workaround.

- CSCsd57076

  Symptoms: A router crashes when you attach a service policy at the PVC level on an ATM interface.

  Conditions: This symptom is observed on a Cisco 7200 series when a bandwidth action is configured in the service policy and when traffic is passing through the interface.

  Workaround: There is no workaround.

- CSCsd64632

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

  3. Symptom 1: After one or two switchovers have occurred, SSH services become disabled because the RSA key is lost.

     Condition 1: This symptom is observed on a Cisco router that functions in either RPR+ or SSO mode.

     Workaround 1: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reconfigure the lost settings via the console or a vty connection.

  4. Symptom 2: After one or two switchovers have occurred, the encrypted SNMP information or private setting becomes lost.

     Condition 1: This symptom is observed on a Cisco router that functions in RPR+ mode.

     Workaround 1: There is no workaround to prevent the symptom from occurring. When the symptom has occurred, reconfigure the lost settings via the console or a vty connection.

- CSCsd87487

  Symptoms: Multilink interfaces remain down after an SSO switchover.

  Conditions: This symptom is observed on a Cisco 10000 series that is configured for LFIoATM or MLPoATM and occurs only when traffic is flowing while an SSO switchover occurs. When there is no traffic, the interfaces come up normally.

  Workaround: There is no workaround.

- CSCsd93555

  Symptoms: On a Cisco 7304 that has an NSE-100, it is possible to configure Link Fragmentation and Interleaving (LFI) over MLP and an egress QoS policy on a multilink interface. This is an inappropriate configuration because neither of these features can work effectively in the NSE-100 architecture.

  Conditions: This symptom is observed on a Cisco 7304 with an NSE-100. Note that LFI over MLP and an egress QoS policy on a multilink interface is an appropriate configuration on a Cisco 7304 with an NPE-G100 and works fine on a Cisco 7304 with an NPE-G100.

  Workaround: Disable LFI over MLP by entering the **no ppp multilink interleave** command. Disable QoS on a multilink interface by entering the **no service-policy output** *policy-map-name* command.

TCP/IP Host-Mode Services

- CSCek01499

  Symptoms: When a CE router that is configured for MPLS reloads, a software-forced crash may occur on the connected PE router because of memory corruption.

  Conditions: This symptom is observed on a Cisco router that functions as a PE router and that has two RPs that function in SSO mode. The symptom does not occur when the router has only a single RP.

  Workaround: There is no workaround.

Wide-Area Networking

- CSCej58338

  Symptoms: A ping may fail across an ISDN BRI channel even though the ISDN B channel is up.

  Conditions: This symptom is observed on a Cisco router when routing protocols are enabled on the ISDN BRI channel.

  Workaround: Clear the BRI B channel.

- CSCek24091

  Symptoms: A PPP session fails to come up, and the following debug message is generated:

  ```
  PPP SSS: stale named authen method list "default"
  ```

  Conditions: This symptom is observed only when a service policy is applied and when the default PPP authentication method list is used.

  Workaround: Use a PPP authentication method list other than the PPP authentication default method list.

- CSCsb71154

  Symptoms: When a VC that is configured under a VP goes down, PPPoE sessions can still be established over the VC.

  Conditions: This symptom is observed on a Cisco 10000 series after you have entered the **shutdown** interface configuration command followed by the **no shutdown** interface configuration command on the main interface or after you have reloaded the router.

  Workaround: There is no workaround.

- CSCsc28120

  Symptoms: A Cisco 7301 may crash when a service policy is removed from an interface that is configured for Frame Relay encapsulation.

  Conditions: This symptom is observed when a service policy is configured on an interface before the encapsulation is changed to Frame Relay. When the service policy is then removed, the router crashes.

  Workaround: Remove the service policy before you change the encapsulation to Frame Relay.

- CSCsd01322

  Symptoms: A PPP session is created with an IP address that is 0.0.0.0.

  Conditions: This symptom is observed on a Cisco router when a RADIUS profile uses the “ip:addr-pool” attribute to assign an IP address and when AAA authorization fails because there is no IP address available in the address pool.

Workaround: Enter the **ppp ipcp address required** command to prevent a PPP session from being created with an IP address of 0.0.0.0.

- CSCsd06110

  Symptoms: A router may exhaust its I/O memory.

  Conditions: This symptom is observed on a Cisco router when you clear 10,000 tunnels on which about 45,000 PPP sessions are established. The symptom occurs only under extreme stress situations.

  Workaround: Clear the tunnels and sessions in stages.

Troubleshooting

The following documents provide assistance with troubleshooting your Cisco hardware and software:

- *Hardware Troubleshooting Index Page*:

  http://www.cisco.com/warp/public/108/index.shtml
- *Troubleshooting Bus Error Exceptions*:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml
- *Why Does My Router Lose Its Configuration During Reboot?*:

  http://www.cisco.com/warp/public/63/lose_config_6201.html
- *Troubleshooting Router Hangs*:

  http://www.cisco.com/warp/public/63/why_hang.html
- *Troubleshooting Memory Problems*:

  http://www.cisco.com/warp/public/63/mallocfail.shtml
- *Troubleshooting High CPU Utilization on Cisco Routers*:

  http://www.cisco.com/warp/public/63/highcpu.html
- *Troubleshooting Router Crashes*:

  http://www.cisco.com/warp/public/122/crashes_router_troubleshooting.shtml
- *Using CAR During DOS Attacks*:

  http://www.cisco.com/warp/public/63/car_rate_limit_icmp.html

Related Documentation

The following sections describe the documentation available for Cisco IOS Release 12.2SB. These documents consist of hardware and software installation guides, Cisco IOS configuration and command reference publications, system error messages, feature modules, and other documents.

Documentation is available online on Cisco.com.

Use these release notes with the following resources:

- Release-Specific Documents, page 964
- Platform-Specific Documents, page 965
- Feature Modules, page 967
- Cisco Feature Navigator, page 967
- Cisco IOS Software Documentation Set, page 967

Release-Specific Documents

This section provides information about release-specific documents.

Cisco IOS Release 12.2SB

For detailed information about release-specific documents for Cisco IOS Release 12.2SB, see the *Cisco IOS Release 12.2SB Documentation Roadmap*:

http://www.cisco.com/en/US/products/ps6566/products_documentation_roadmap09186a00806786c3.html

Configuration guides, command references, system message guides, product bulletins, field notices, and other release-specific documents for Cisco IOS Release 12.2SB are located on Cisco.com and at http://www.cisco.com/en/US/products/ps6566/tsd_products_support_general_information.html:

Cisco IOS Release 12.2

The following documents are specific to Cisco IOS Release 12.2 and are located on Cisco.com and at http://www.cisco.com/univercd/home/index.htm:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2:*
- Configuration guides, command references, system message guides, product bulletins, field notices, and other release-specific documents:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/tsd_products_support_eol_series_home.html
- Caveats for Cisco IOS Release 12.2 (Parts 5 through 8)

  As a supplement to the caveats listed in the "Caveats" section in these release notes, see the *Cross-Platform Release Notes for Cisco IOS Release 12.2*, which contain caveats applicable to all platforms for all maintenance releases of Release 12.2:

  Cross-Platform Release Notes for Cisco IOS Release 12.2:

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Support: Tools & Resources: Bug Toolkit** (which is listed under Troubleshooting). Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

Cisco IOS Release 12.2S

The following documents are specific to Cisco IOS Release 12.2S and are located on Cisco.com and at http://www.cisco.com/univercd/home/index.htm:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2S*

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 S**: **Release Notes**

  On http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **Release Notes**

- New Feature Documentation

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 S**: **Feature Guides**

  On http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **New Feature Documentation**: **Cisco IOS Release 12.2 S**: **New Feature Documentation**

- Configuration guides, command references, system message guides, product bulletins, field notices, and other release-specific documents

  On Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 S**

  On http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **New Feature Documentation**: **Cisco IOS Release 12.2 S**: **System Messages for 12.2S**

Platform-Specific Documents

Platform-specific information and documents for the platforms that are supported in Cisco IOS Release 12.2SB are available at the locations listed below:

- Cisco 7200 Series Routers
  - Cisco 7200 series home page on Cisco.com at

    Products & Services: **Products: Routers and Routing Systems**: **7200 Series Routers**

  - Cisco 7200 series technical documentation on Cisco.com at

    Products & Services: **Products: Routers and Routing Systems**: **7200 Series Routers**: in the "Technical Documentation & Tools" box on the right of the page, **Cisco 7200 Series Routers**

    For Cisco 7200 series technical documentation on http://www.cisco.com/univercd/home/index.htm, select a Cisco 7200 series router from the **Routers** pull-down menu on the top left of the page.

- Cisco 7301 Router
  - Cisco 7300 series home page on Cisco.com at

    Products & Services: **Routers & Routing Systems**: **All Routers & Routing Systems**: **Cisco 7300 Series Routers**

  - Cisco 7300 series technical documentation on Cisco.com at

    Products & Services: Routers & Routing Systems: **All Routers & Routing Systems**: **Cisco 7300 Series Routers**: in the "Technical Documentation & Tools" box on the right of the page, **Cisco 7300 Series Routers**

  - Cisco 7301 technical documentation on http://www.cisco.com/univercd/home/index.htm at

    Routers: **Cisco 7301**

- Cisco 7304 Router
  - Cisco 7300 series home page on Cisco.com at

    Products & Services: **Routers & Routing Systems**: **All Routers & Routing Systems**: **Cisco 7300 Series Routers**

  - Cisco 7300 series technical documentation on Cisco.com at

    Products & Services: Routers & Routing Systems: **All Routers & Routing Systems**: **Cisco 7300 Series Routers**: in the "Technical Documentation & Tools" box on the right of the page, **Cisco 7300 Series Routers**

  - Cisco 7304 technical documentation on http://www.cisco.com/univercd/home/index.htm at

    Routers: **Cisco 7304**

- Cisco 10000 Series Routers
  - Cisco 10000 series home page on Cisco.com at

    Products & Services: **Routers & Routing Systems**: **All Routers & Routing Systems**: **Cisco 10000 Series Routers**

  - Cisco 10000 series technical documentation on Cisco.com at

    Products & Services: **Routers & Routing Systems**: **All Routers & Routing Systems**: **Cisco 10000 Series Routers**: in the "Technical Documentation & Tools" box on the right of the page, **Cisco 10000 Series Routers**

  - Cisco 10000 series technical documentation on http://www.cisco.com/univercd/home/index.htm at

    Routers: **Cisco 10000 ESR**

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2SB and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature modules for Cisco IOS Release 12.2SB are available at the following locations:

- Release 12.2(31)SB2

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb31/index.htm
- Release 12.2(28)SB

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122sb/newft/122sb28/index.htm

Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS and Catalyst OS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Cisco IOS Software Documentation Set

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

Documentation Modules

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

- Configuration guides on Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**: **Reference Guides**: **Configuration Guides**
- Command references on Cisco.com at

  Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**: **Configure**: **Command References**

- Configuration guides and command references on http://www.cisco.com/univercd/home/index.htm at

  Cisco IOS Software: **Release 12.2**: **Cisco IOS Release 12.2 Configuration Guides and Command References**

Cisco IOS Release 12.2 Documentation Set Contents

Table 1 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in electronic form and in printed form if ordered.

Note You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On Cisco.com at

Support: **Documentation**: **Cisco IOS Software**: **Cisco IOS Software Releases 12.2 Mainline**

On http://www.cisco.com/univercd/home/index.htm at

Cisco IOS Software: **Release 12.2**

Modules	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Cisco IOS User Interfaces File Management System Management
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2* • *Cisco IOS Bridging and IBM N2etworking Command Reference, Volume 2 of 2*	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSW+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server

Modules	Major Topics
- *Cisco IOS Dial Technologies Configuration Guide* - *Cisco IOS Dial Technologies Command Reference*	Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Point-to-Point Protocols Dial-on-Demand Routing Dial Backup Dial Related Addressing Service Network Access Solutions Large-Scale Dial Solutions Cost-Control Solutions Internetworking Dial Access Scenarios
- *Cisco IOS Interface Configuration Guide* - *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
- *Cisco IOS IP Configuration Guide* - *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services* - *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* - *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*	IP Addressing IP Services IP Routing Protocols IP Multicast
- *Cisco IOS AppleTalk and Novell IPX Configuration Guide* - *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk Novell IPX
- *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide* - *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
- *Cisco IOS Voice, Video, and Fax Configuration Guide* - *Cisco IOS Voice, Video, and Fax Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
- *Cisco IOS Quality of Service Solutions Configuration Guide* - *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms

Modules	Major Topics
- *Cisco IOS Security Configuration Guide* - *Cisco IOS Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
- *Cisco IOS Switching Services Configuration Guide* - *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
- *Cisco IOS Wide-Area Networking Configuration Guide* - *Cisco IOS Wide-Area Networking Command Reference*	ATM Frame Relay SMDS X.25 and LAPB
- *Cisco IOS Mobile Wireless Configuration Guide* - *Cisco IOS Mobile Wireless Command Reference*	General Packet Radio Service
- *Cisco IOS Terminal Services Configuration Guide* - *Cisco IOS Terminal Services Command Reference*	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
- *Cisco IOS Configuration Guide Master Index* - *Cisco IOS Command Reference Master Index* - *Cisco IOS Debug Command Reference* - *Cisco IOS Software System Error Messages* - *New Features in 12.2-Based Limited Lifetime Releases* - *New Features in Release 12.2 T* - *Release Notes* (Release note and caveat documentation for 12.2-based releases and various platforms)	

Note *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco.com. From Cisco.com, click the following path: **Support: Software Downloads: Network Management Software: Cisco Network Management Toolkit:** Cisco MIBs.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Original SSLeay License:

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 964.

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