Caveats for Cisco IOS Release 12.2(31)SB15 through 12.2(33)SB2

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

Open Caveats—Cisco IOS Release 12.2(33)SB2

Cisco IOS Release 12.2(33)SB2 is a rebuild release for Cisco IOS Release 12.2(33)SB. This section describes a severity 2 caveat that is open in Cisco IOS Release 12.2(33)SB2. There are other open caveats in Cisco IOS Release 12.2(33)SB2. However, open caveats are normally listed only for maintenance releases, and the listing of CSCsu81943 is an exception.

- CSCsu81943

  Symptoms: Packet buffering is happening on the ATM line card in the transmit direction. Packets get dropped at LC with “No buffer” as reason in the transmit direction. This causes latency and packet drops for PQ and non-PQ traffic.

  Conditions: The issue occurs when traffic sent to the VC is higher than what VC can support.

  Problem is specific to ATM line cards with vbr-nrt configuration and on PRE-4. And the problem is seen only when traffic per-vc is high enough to cause buffering at LC. Problem happens only if the traffic is continuous and high. If the traffic is bursty, then between bursts, there may be enough time for the LC to drain packets, and we will not experience high latency.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SB2

Cisco IOS Release 12.2(33)SB2 is a rebuild release for Cisco IOS Release 12.2(33)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SB2 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCsa98164

  Symptoms: When the **boot config** *file-system-prefix filename* **nvbypass** command is enabled, no file is created on a secondary Route Processor (RP).

  Conditions: This symptom is observed on a Cisco 10000 series that is configured with two PREs that function in RPR+ mode but may also occur on other platforms that are configured with redundant RPs.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsj35342

  Symptoms: When AAA gigabyte counter support is enabled, it is possible for the AAA HC Counter process to consume significant CPU.

  Conditions: This symptom occurs when AAA gigabyte counter support is enabled.

  Workaround: Configure “no aaa accounting gigawords.”

- 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.

- 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.

- 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.

- 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.

- CSCsk94713

  Symptoms: With traffic engineering tunnels configured on a NSE-100 router with PXF enabled, the packets are following IP path instead of MPLS tunnel path. The core interface of the LSP identifies the packets as IP packets instead of MPLS packets.

  Conditions: This symptom occurs when traffic engineering tunnel source is a NSE-100 router.

  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.

- CSCsl65327

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

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

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

- CSCsl86316

  Symptoms: High CPU utilization and tracebacks occurs in the VTEMPLATE Backgr process of the VPDN subsystem and may result in the router becoming unstable.

  Conditions: The symptoms are observed in an L2TP scenario

  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.**

- 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.

- 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.

- CSCsm23560

  Symptoms: OSPF TE tunnel does not replace the existing route, which can be verified using the **show ip route** command.

  Conditions: The symptom is observed when using the **mpls traffic-eng multicast-intact** command so that PIM and MPLS-TE can work together in OSPF. The tunnel route will be established but it will not replace the existing ethernet route.

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

  Alternate workaround: Do not use the **mpls traffic-eng multicast- intact** command, so that PIM and MPLS-TE do not work together and OSPF tunnel is able to replace the route.

- 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.

- CSCsm48574

  Symptoms: The following error message and traceback are observed:

```
Jan 31 12:51:12.357 EST: %HQF_MAP_TT-3-HQF: hmt_logical_queue_reparent
 error
    detected: Old/New parent combination not supported 0x6 0x6
```

  Conditions: When a queuing policy-map is applied to a L2TP session at the LNS, if the L2TP tunnel is shifted from one interface to another interface, the error message will be seen.

  Workaround: Avoid situations where the physical interface shifts at the L2TP LNS from one interface to another, even by routing updates which force the L2TP tunnel to come into the LNS by another interface. Using a loopback interface as the tunnel end point does not prevent the error.

- CSCsm54873

  Symptoms: Embedded Event Manager (EEM) rules may not trigger properly when performing SIP OIR.

  Conditions: EEM policies that interact with the IOS CLI through the **command action** command and EEM TCL policies that use the CLI library may not interact properly when triggered. Incorrect sequencing with the IOS CLI may result when the policies are triggered resulting in the Cisco IOS CLI commands not being invoked.

  This problem exists on all shipped versions of IOS XE.

  Workaround: There is no workaround.

  Further Problem Description: This can impact customers that use the Embedded Event Manager with EEM applets or policies that interact with the CLI.

  It was seen on the ASR platform and other platforms when “sched heapchecks process” was enabled. A timing issue can cause EEM action CLI commands to not coordinate with the IOS exec properly.

  The SIP2 is probably related to the ASR platform. An OIR event is used to trigger the specific EEM policy. This should occur with any EEM type policy however.

  SXF is not impacted by this bug.

- 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.

- CSCsm73602

  Symptoms: High CPU load due to VTEMPLATE Backgr process.

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

  Workaround: There is no workaround.

- CSCsm78539

  Symptoms: PPPoE sessions may fail to establish with the following error: “Failed to insert into remote lookup database”.

  Conditions: The symptom is observed with a large number of VPDN tunnels.

  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.

- CSCso26940

  Symptoms: The following error messages may appear on a router when bringing up PPPoX sessions, and the router will not be able to establish new sessions:

  ```
  %AAA-3-ACCT_LOW_MEM_UID_FAIL: AAA unable to create UID for incoming calls
  due
   to insufficient processor memory
   %AAA-3-LOW_MEM:  Author process is unable to handle the incoming packet due
   to low memory
  ```

  Condition: This is seen when a large number of PPPoE sessions (approximately 32000) are attempted, with edge configuration + traffic classes using radius-based authentication. Only up to 29000 sessions may come up before hitting the above error.

  Workaround: There is no workaround.

  Further Problem Description: This is a scalability issue related to PRE2 only.

- CSCso29724

  Symptoms: With negative RemotePort feature, the Gigabit on Provider Edge 1 (PE1) goes down after second switchover on PE1.

  Conditions: The Gigabit used on PE1 is FHGE. The Gigabit on PE1 goes down after switchover with negative RemotePort feature configured.

  Workaround: Do a **shut** and **no shut** in primary after every switchover.

- 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.

- CSCso39518

  Symptoms: Traceback displayed on the console.

  Conditions: Before applying patch with Cisco IOS Embedded Event Manager (EEM) policy dir subsystem in it, there is one or more EEM applets configured, after the patch is activated, trigger an EEM applet.

  Workaround: Unconfigure all the EEM applets before patching, then apply all the EEM applets after activating the patch.

  Further Problem Description: This would lead to (fh_policy_dir.proc)process crash, not a device crash. This bug is specific to modular Cisco IOS image.

- CSCso42695

  Symptoms: A few member links may fail to come up as an MLP bundle, after issuing the **hw module reset** command on a CPE or otherwise issuing the **clear vpdn tun l2 all** command on the LNS in UP MLPoLNS setup.

  Conditions: The symptoms are observed when scaling configurations (2040 bundles with five member-links each).

  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.

- CSCso51661

  Symptoms: OSPF process may show a high CPU load after graceful shutdown of the OSPF process.

```
router ospf 1
 shutdown
```

Conditions: This symptom occurs after graceful shutdown of the OSPF process.

Workaround: Do not use OSPF Graceful Shutdown feature in affected Cisco IOS versions.

- CSCso56644

  Symptoms: There will be a CPU hog message displayed on the console.

  Conditions: This symptom is seen when over 800 EEM applets or Tcl policies are configured. Then turn on **debug event manager** command.

  Workaround: Configure less than 800 EEM policies during debugging EEM.

- 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.

- CSCso67195

  Symptoms: Router may crash due to memory corruption:

```
%SEC-6-IPACCESSLOGRP: list 111 denied pim 0.0.0.0 ->
 <removed>, 1 packet


%SYS-2-CHUNKBADMAGIC: Bad magic number in chunk header,
 chunk 680A5374  data 680A79A4  chunkmagic FFFFFFFF  chunk_freemagic 0 -
 Process= "Mwheel Process", ipl= 0, pid= 274,  -Traceback= 0x6169C450
 0x60102E78 0x601031E4 0x61D418E4 0x61D4230C 0x61CF1A48 0x61D1280C 0x61D05FE4
 0x61D0E9FC

 chunk_diagnose, code = 1

 chunk name is PIM JP GroupQ
```

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

```
ip pim sparse-dense-mode
access-list 98 deny any log
```

Workaround: Remove access-list logging.

- CSCso71742

  Symptoms: The following errors are observed on the Cisco 10000 new Active PRE after HA cutover:

  ```
  %GENERAL-3-EREVENT: NULL swidb
  ```

  Conditions: The error occurs on a Cisco 10000 PRE when the PRE becomes active following an ISSU upgrade and an HA failover of the PRE. This error also has been observed with ISSU process.

  Workaround: There is no workaround. At this point it is not clear the impact of these errors on the system.

- CSCso74257

  Symptoms: Memory leaks may be seen.

  Conditions: The symptoms are observed when running Cisco IOS Release 12.2S and when QoS is configured for ISG IP sessions.

  Workaround: There is no workaround.

- 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.

- CSCso87916

  Symptoms: Router may crash when booting with large number of interfaces configured for RIP for IPv6 (RIPng).

  Conditions: Occurs when RIPng is configured on 1000 or more interfaces.

  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.

- CSCso92930

  Symptoms: Available memory may decrease over time on a Cisco ASR1000 RP as subscribers connect and disconnect.

  Conditions: This symptom is observed when the Cisco ASR1000 functions as a LAC or LNS. AAA accounting is enabled for tunnel, session and PPP.

  Workaround: If the available memory decrease impacts system functions, disable AAA accounting as a temporary remedy.

- CSCsq04673

  Symptoms: A switch running Cisco IOS Release 12.2(33)SXH1 may show a SIGSEGV error.

Conditions: The symptom is observed when EEM policies are configured. The issue will take effect when both: a) An EEM policy with event syslog is executed; and b) The system does not have any memory left.

Workaround: There is no workaround.

Further Problem Description: The issue is not specific to ION images as IOS images are also impacted. It is not platform specific.

- CSCsq07229

  Symptoms: Real interface (non-vtemplate) L4Redirect configuration may not be applied to interface subscriber sessions.

  Conditions: The symptoms are specific to interface subscriber sessions with L4Redirect configured on the interface.

  Workaround: Configure L4Redirect within a service profile and use a control policy map on the interface to apply the service profile at the session start.

- 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.

- 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.

- CSCsq17712

  Symptoms: ISSU process does not automatically rollback to the previous version.

  Conditions: This symptom occurs after rollback timer has expired in RPR mode.

Workaround: There is no workaround.

- CSCsq18756

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

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

  Workaround: There is no workaround.

- 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.

- CSCsq21589

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

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

  Workaround: Reload the router that is running ISG.

- 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.

- CSCsq30401

  Symptoms: After a switchover, multilink bundles may fail to come up.

  Conditions: This symptom is observed on platforms that support High Availability (HA) such as a Cisco 7600 series or 10000 series router, and is triggered by an error in synchronizing the state of the multilink bundle to the standby processor.

  Workaround: The only workaround, short of reloading the processor, is to remove the multilink interface from the configuration with the **no multilink interface** command and then adding it back.

- 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.

```
%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:

```
FIBrp_xdr: Table IPv4:<vrf name>, building insert
 event xdr for x.x.x.x/y. Sources: RIB
FIBrp_xdr: Encoding path extensions ...
FIBrp_xdr:  - short ext, type 1, index 0
FIBrp_xdr: Getting encode size for IPv4 table broker
 FIB_FIB xdr
:    - short path ext: len 12
:    - short path ext: len 24
:    - feat IPRM, len 12
:  => 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.

- CSCsq31958

  Symptoms: In a network with redundant topology, an Open Shortest Path First (OSPF) external route may remain stuck in the routing table after a link flap.

  Conditions: Problem observed in Cisco IOS Release 12.4T. Not present in Cisco IOS Release 12.3T.

  Workaround: The issue can be resolved by entering the **clear ip route** command for the affected route.

- CSCsq37834

  Symptoms: Peruser QoS may not be applied to a session via a CoA push.

  Conditions: The symptom occurs only when a QoS policy (in/out/both) is pushed onto a session. If other ISG features are pushed along with the QoS policy, the problem is not seen.

  Workaround: There is no workaround.

- CSCsq43591

  Symptoms: When a session is cleared from the CPE and when it reconnects instantaneously, a ping fails to the CPE.

  Conditions: This symptom is observed under the following conditions:

  - LAC<->LNS setup.
  - Clearing of session from CPE.
  - In the **show pxf cpu vcci** command output, there is no VCCI present for the VAI.
  - Also seen in lab when the CPE is booted and the first session comes up.

  Workaround: Clear the VAI interface from the LNS. The session will reconnect and will work fine.

- CSCsq43678

  Symptoms: A Cisco 7300 NSE may experience multiple unexpected reloads due to an address error.

  Conditions: The symptom is observed with QOS configuration policing on the outbound traffic. Running output policer on a packet that has not been classified causes the unexpected reload.

  Workaround: There is no workaround.

- CSCsq43831

  Symptoms: A Cisco IOS router may unexpectedly reload when Forwarding Information Base (FIB) processes an adjacency for route that has many levels of recursion.

  Conditions: This has only been seen after the following error message was displayed:

  ```
  %COMMON_FIB-6-FIB_RECURSION: 10.10.10.1/32 has too many (8) levels of
  recursion during setting up switching info
  ```

  Workaround: Change static routes so they specify both the interface and next-hop instead of just specifying the next-hop. For example change:

  ```
  ip route 10.0.0.0 255.255.255.255 192.168.1.1
  to
  ip route 10.0.0.0 255.255.255.255 GigabitEthernet1/0 192.168.1.1
  ```

  This is particularly true when using eBGP between loopbacks to allow for multiple parallel links between the two eBGP peers, where one typically installs static routes for the eBGP peers address. Make sure these static routes have both interface and next-hop specified.

- CSCsq44598

  Symptoms: A PA-POS-2OC3 experiences an output stuck condition.

  Conditions: This issue is sporadic in nature and is sometimes seen with QoS configurations although QoS is not the cause of the issue. The issue is due to an extra interrupt, which is confusing the driver if it expires before the FIFO reaches the low point. For example, if the FIFO goes full but is filled with large packets, then it is possible that the no traffic timer will expire before the tx packets have emptied. It is a communication issue between the hardware and the driver code.

  Workaround: There is no workaround.

- CSCsq44823

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

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

  Workaround: There is no workaround.

- CSCsq48201

  Symptoms: A crash may occur when creating a Bridge-Group Virtual Interface (BVI) while traffic is flowing.

  Conditions: The crash could occur when a BVI interface is first created with the command **interface BVI** and traffic is being process switched by a physical interface in the same bridge-group. Once the BVI interface is created, subsequent **interface BVI** commands to configure that interface will not cause the crash.

  Workaround: Remove the physical interface from the bridge-group, or prevent traffic from being process switch by the interface when the BVI interface is first created.

- 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.

- CSCsq52048

  Symptoms: Router crashed while running **show vpdn tunnel all** command.

  Conditions: When there are thousands of L2TP tunnels coming up, going down, running **show vpdn tunnel all** may result in crash.

  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.

- CSCsq60073

  Symptoms: An OSPF router process may experience high CPU load, after shutting down the OSPF graceful shutdown process.

  Conditions: The symptom is observed if the OSPF graceful shutdown is configured together with MPLS TE.

  Workaround: Do not shutdown the OSPF process when configured for MPLS TE.

- CSCsq62653

  Symptoms: A router may crash if the **show subscriber** command is executed on the VTY followed by a clearing of the main session.

  Conditions: The symptom is observed if the **show subscriber** command is executed on the VTY followed by a clearing of the main session.

  Workaround: Use the **show subscriber** command only on the main TTY.

- 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.

- CSCsq69178

  Symptoms: ISSU fails, and the standby continuously reloads.

  Conditions: The symptom is observed when trying to perform an ISSU upgrade.

  Workaround: There is no workaround.

- CSCsq70055

  Symptoms: The standby RP may fail to boot by either dropping back to rommon, or by attempting to boot multiple times.

Conditions: The symptoms are observed on the standby RP with the same Cisco IOS Release on the Active RP. However, it is more likely this problem will be seen during ISSU with different Cisco IOS Releases.

Workaround: There is no workaround.

- CSCsq70980

  Symptoms: When terminating 32,000 PPPoEoQinQ PTA sessions, none of the sessions are flagged as PTA on the standby processor. All sessions are perpetually flagged as Transient.

  Conditions: The symptoms are observed on a Cisco 10000 series router running dual PRE processors in SSO mode. The PTA sessions are PPPoEoQinQ, and properly authenticated and terminated on the active PRE. The sessions are left in transient state on the standby PRE. In each case, the AAA configuration uses AAA groups for authentication and AAA accounting. Routers showing this issue have the throttling access command present in the AAA groups. The following command is used to observe the issue (issue the command on both the active and standby processors): **show pppoe summary**.

  Workaround: If the throttle access command is not present in the AAA groups, standby synchronization of PTA sessions occurs as desired. Remove the throttle access with the following command sequence: **config t aaa group server radius AUTHEN-SERVERS default throttle access 50 end**

- CSCsq73727

  Symptoms: An ISG router may crash during ISG-SCE negotiation, if there are missing or invalid values for the version EPD attributes.

  Conditions: The symptom is observed on an ISG router during ISG-SCE negotiation.

  Workaround: Use an SCE version that is within the valid range.

- 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.

- CSCsq75705

  Symptoms: An OC3ATM line card sends 32 event messages.

  Conditions: This symptom occurs when the standby router takes over.

  Workaround: There is no workaround.

- CSCsq77043

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

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

  Workaround: Reduce the size of the hostname.

- 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.

- CSCsq79457

  Symptoms: Pings fail from CPE to the bundle peer address on LNS.

  Conditions: This symptom can occur whenever MLP on LNS is configured.

  Workaround: There is no workaround.

- CSCsq80589

  Symptoms: During a maintenance window, a Cisco 7206VXR router is upgraded from an NPE-G1 to an NPE-G2. The router comes up normally after the swap, but about 10 minutes later the router crashes. When it comes up again, the configuration is checked, but the router crashes again.

  The following error message is seen:

  ```
  "Unexpected reboot due to SegV Exception" (as indicated by show version)
  ```

  Conditions: This symptom is observed when upgrading a Cisco 7206VXR from an NPE-G1 to an NPE-G2.

  Workaround: There is no workaround.

- CSCsq81235

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

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

  Workaround: There is no workaround.

- CSCsq84757

  Symptoms: When ERSPAN is configured on active RP of an ASR, the configuration may not be correctly synced to standby RP.

  Conditions: This problem happens when ERSPAN configuration is the last configuration line in NVRAM.

  Workaround: This has been fixed and is not ERSPAN issue. Instead it is a generic config-bulk sync issue.

- 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.

- CSCsq91348

  Symptoms: There may be a crash during a service/user-profile authorization when removing taps through SNMP.

  Conditions: The symptom is observed when making a service/user-profile authorization while removing a tapfile through SNMP.

  Workaround: If possible, do not make authorizations when removing taps through SNMP.

- 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.

- CSCsr00973

  Symptoms: When a router is in redundant mode, some start-up configurations are missing on standby RP after save configuration.

  Conditions: This symptom occurs when “boot config bootflash:*filename*” is configured and save configuration via the **copy run start** command or the **write memory** command. It does not occur with save to default setting. (Save in NVRAM.) Check that configurations are missing by “Router#more stby- bootflash:router-config”.

  Workaround: Use the **copy run stby-bootflash:** *filename* command.

- 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.

- 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.

- CSCsr06699

  Symptoms: On a Cisco 10000 PRE-4 with GigabitEthernet SPA, ping fails across port-channel interface with dot1q/QinQ subinterfaces defined.

  Conditions: This symptom is observed on 1+N port-channel interface with the following conditions:

  i) do1q subinterfaces (VLANs) or QinQ subinterfaces (stacked VLANs) defined.

  ii) IP address configured on the subinterfaces.

  Workaround: Perform a microcode reload.

  Further Problem Description: This is seen on both PRE-3 and PRE-4 with GE SPA combination. The same problem is not observed with legacy GE card (HH-GE and FH-GE) combinations.

- CSCsr07125

  Symptoms: Local Switching is not passing traffic after LC reload, multiple switchover, or unconfigure/reconfigure “connect” CLIs on a Local Switching.

  This issue will be hit only on scaled testbed where mac_rewrite_index will go beyond 16 bits.

  Conditions: This symptom occurs after LC reload, multiple switchover, or unconfigure/reconfigure “connect”.

  Workaround: Toggle the “connect” by removing and reconfiguring it (note: even though this is a step that triggers the problem in the beginning, it also fixes it as it requires the encap string to be reprovisioned).

- CSCsr10075

  Symptoms: Under very rare timing condition, an OSPF Type-5 route may stay in the routing table after the adjacency is lost over ISDN/virtual-access interface.

  Conditions: The problem is seen only in Cisco IOS versions that do not have integrated CSCeh23420. Cisco IOS versions with CSCeh23420 are not affected.

  Workaround: Clear IP route for the route, which is stuck in the routing table. Upgrade to a Cisco IOS version that are integrated with CSCeh23420 or CSCsr10075.

- 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.

- CSCsr19228

  Symptoms: When adding a subinterface, the console has error message and traceback.

  For Cisco IOS Release 12.2(33)SB, there is only a traceback on standby console:

```
%HA-4-DECODE: Failed to decode channelized hwidb (4, 0, 0, 0)
-Traceback= 403FE9F8 40480438 40436AA8 4043586C 40434F74 40431F5C 4042C810
```

  For Cisco IOS Release 12.2(31)SB12, both active and standby console:

```
Acitve:
Router(config)#controller SONET 4/0
Router(config-controller)#au-4 1 tug-3 1
Router(config-ctrlr-tug3)#tug-2 2 e1 3 unframed
Router(config-ctrlr-tug3)#
1d02h: IDB Sync: Interface Serial4/0.1/1/2/3:0, oldstate=0, state=0,
onintstack=0
1d02h: Sending message for interface Serial4/0.1/1/2/3:0, state = 0, oldstate
= 0 idbsync_only = 1
1d02h: Syncing tifnum (22) for interface Serial4/0.1/1/2/3:0 (key 40000050000
attr 0x1)
1d02h: %STANDBY-3-MSG:
00:57:20: %NETWORK_RF_API-3-FAILDECODEDATADESC: Cannot decode data descriptor
for an interface or controller because the sync header cannot be decoded,
descriptor type=1
-Traceback= 40310C48 40310E68 402E33A0 402E0F34 402DE378 402D8954
1d02h: NETWORK: No sync for Serial4/0.1/1/2/3:0 oldstate=0, state=0
1d02h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial4/0.1/1/2/3:0,
changed state to down
Router(config-ctrlr-tug3)#

Standby:
Router#
00:57:20: CH-STM1 4/0 decoded (4, 0, 0, 5)
00:57:20: %HA-4-DECODE: Failed to decode channelized hwidb (4, 0, 0, 5)

-Traceback= 402FDE04 403106F8 40310E68 402E33A0 402E0F34 402DE378 402D8954
00:57:20: %NETWORK_RF_API-3-FAILDECODEDATADESC: Cannot decode data descriptor
for an interface or controller because the sync header cannot be decoded,
descriptor type=1
-Traceback= 40310C48 40310E68 402E33A0 402E0F34 402DE378 402D8954
00:57:20: Hashed the tifnum 22 at address 1968 (count 1, key 40000050000)
00:57:20: Found the Tifnum 22 at the address 1968(count 1, key 40000050000,
```

```
attr 0x1, cardtype 0x3C3 subcardtype 0x321)
00:57:20: Sby tif no. for port Serial4/0.1/1/2/3:0 (key 40000050000, attrib
0x1, cardtype 0x3C3, subcardtype 0x321): 22
```

Conditions: This symptom is observed on a Cisco 7304 with two NPE-G100s in SSO mode.

Workaround: Disable SSO redundancy.

- CSCsr38553

  Symptoms: An OBFL VOLT bootflash every 5 minutes is taking the CPU to 60%.

  Conditions: This symptom is observed when background process OBFL VOLT bootflash takes the CPU to 60% every 5 minutes.

  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.

- 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.

- CSCsr43461

  Symptoms: Some configurations are missing after a reload.

  Conditions: This symptom is seen when a router reloads that results in missing configurations of “vrf selection source” under show run.

  Workaround: There is no workaround.

- CSCsr43895

  Symptoms: If the **crypto key generate rsa** command is executed on a redundant system and the system fails over to the standby, the RSA keys will not be propagated to the new primary.

  Conditions: This symptom is observed on redundant PREs that must be set up with SSH RSA keys using the **crypto key generate rsa** command on the primary.

  Workaround: After failover, execute the **crypto key generate rsa** command on the new primary PRE.

- CSCsr50280

  Symptoms: A PRE2 to PRE4 upgrade results in config sync issues: running config on PRE2 is not synced to the standby PRE4.

  Conditions: This symptom occurs when PRE2 HA setup is being upgraded to PRE4, by replacing standby PRE2 with PRE4, and then performing redundancy force switchover.

Workaround: Copy the running config from Active PRE[PRE2] to a disk0/1, and then use the disk to copy the configs on the stby PRE[PRE4].

- 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.

- CSCsr57502

  Symptoms: Tracebacks appear when we create subinterfaces for SONET of different slots on a Cisco 7304 router with two NPE-G100s that are running in SSO mode.

  Conditions: This is observed when slot number is not assigned to the IDB as part of the identity. So two subinterfaces of different slots will have the same identity which implies two subinterface IDBs will have the same ifindex number.

  Workaround: Update the slot number in IDB so that the slot number will be part of IDB identity, and the two subinterfaces will have different ifindex numbers.

- 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.

- CSCsr70963

  Symptoms: A Cisco 10000 PRE will reload unexpectedly when a radius server which is marked as dead is removed from the configuration during authentication of sessions.

  Conditions: The issue is seen when a RADIUS server is marked as dead. There are attempts to retry and access the server during its removal from the configuration.

  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.

- CSCsr82003

  Symptoms: With a setup that has two routers receiving the same 300 multicast traffic from a video headend, if one of the links to the headend fails, about half of the multicast groups are blacked out as the RPF information for some of the sources is set wrong. Additionally, if both of the links are lost, we still have entries in the multicast routing table as the alternate route is used as the traffic incoming interface.

  The IGP is OSPF, with area0 in the core, and area 1 (to be set to stub soon) on the headend connecting links. There is MPLS TE with multicast-intact command under OSPF on the routers.

  Conditions: The problem happens when one of the headend connecting links is lost.

  Workaround: Remove the **ip multicast multipath** command from the two routers to disable ECMP load-splitting.

- CSCsr83156

  Symptoms: Bidirectional traffic flows will be stopped on MLPoATM bundle.

  Conditions: This symptom occurs when any of following conditions occur:

  1. Hw-module-reset on the card. 2. ATM main interface the **shut** command followed by the **no shut** command. 3. Member link subinterface the **shutdown** command followed by the **no shutdown** command.

  Workaround: Remove the multilink interface and configure again, or issue the **shut** command followed by the **no shut** command on the bundle.

- CSCsr85093

  Symptoms: SSH connection fails to establish after SSO with the following debug message on client side:

  ```
  SSH2 CLIENT 0: RSA signature verification failed, status 524
  ```

  Conditions: This symptom occurs when a new RSA key is generated. The SSH server key is not updated on the standby. The **show ip ssh** command on the standby will show that SSH is enabled, but the SSH connection will fail to establish.

  Workaround: Regenerate RSA key on the new active after SSO.

- CSCsr88389

  Symptoms: IPv6 neighbor discovery for link-local address fails due to SSO switchover.

  Condition: This symptom is observed when SSO switchover occurs.

  Workaround: Disabling and reenabling IPv6 CEF process will fix the issue.

- 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.

- CSCsu00221

  Symptoms: Deleting the ATM subinterface on a DS3ATM line card causes a router to crash.

  Conditions: This symptom occurs after changing the dsx3mode from plcp to adm or vice versa.

  Workaround: There is no workaround.

- CSCsu01372

  Symptoms: If “boot config disk0:*filename* nvbypass” is used, the startup configuration does not get sync to standby RP after the router reloads.

  Conditions: This symptom occurs if “boot config disk0:*filename* nvbypass” is used.

  Workaround: Issue the **write memory** command after the router reloads.

- 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 queuing 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.

- CSCsu27752

  Symptoms: Using the **shut** command followed by the **no shut** command on an ATM local switch connection can cause the following:

  ```
  %ALIGN-3-SPURIOUS: Spurious memory access made at
  0x417ECDBC reading 0x0
  %ALIGN-3-TRACE: -Traceback=
   417ECDBC 417ED2DC 4194E6FC 41048494 41048524 4104F944 4194E820 417ED3AC
  ```

  Conditions: This symptom is observed on an ATM local switch connection.

  Workaround: There is no workaround.

- CSCsu37038

  Symptoms: Traffic issue is seen with ATM test cases.

  Conditions: This symptom is seen with VBR. Traffic issue is seen for ATM test cases with oversubscription.

  Workaround: There is no workaround.

- CSCsu56541

  Symptoms: Active crashes when issuing **no card 8/2** command.

  Conditions: This symptom occurs during normal conditions of router. This is seen on all PRE types in Cisco IOS Release 12.2(33)SB.

  Workaround: There is no workaround.

- CSCsu68703

  Symptoms: A router crashes when doing a no card on ATM line card.

Conditions: This symptom is observed when doing a no card on ATM line card.

Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SB1

Cisco IOS Release 12.2(33)SB1 is a rebuild release for Cisco IOS Release 12.2(33)SB. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SB1 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCdv07156

  Symptoms: A router that is configured with thousands of RIP routes may crash when multiple links flap.

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

  Workaround: There is no workaround.

- CSCdy22725

  Symptoms: The sustainable cell rate (SCR) value is lost and becomes zero when you reset an interface under which a permanent virtual connection (PVC) is defined with the old style syntax and that has variable bit rate (VBR) traffic parameters. The same PVC disappears completely from the configuration after the router is rebooted.

  Conditions: These symptoms are observed on a Cisco 7500 series router.

  Workaround: Use the new style syntax to define the PVC.

- 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.

- CSCed88426

  Symptoms: An extended ACL applied on an interface does not permit/deny traffic as expected on the standby after switchover.

  Conditions: This symptom is observed when the user does ACL configuration using ACL submode and types Ctrl-C. This causes the config mode to be exited on active, but the command line synced to standby is “\0”. Nothing gets executed on standby, and the ACL submode exit handler is not called. If switchover happens, ACL configuration becomes out of sync. This happens only at the first switchover. Subsequent switchovers do not show this issue.

  Workaround: Avoid the use of Ctrl-C in any of the config modes. Use the **exit** or **end** command instead.

- CSCef15846

  Symptoms: There are two symptoms which are fixed by this bug.

  Symptom 1: When the last peer of a peer-group that is defined in a VRF address- family is deleted, the peer-group configuration will also disappear if no policy is configured for the peer-group.

Condition 1: This symptom is observed in a customer configuration modification.

Workaround 1: Configure a policy for the peer-group such as a route-map.

Symptom 2: Peer-group that is used exclusively by IPv6 peers is activated under the IPv4 address-family.

```
sho configuration  | b address-family ipv4
address-family ipv4
neighbor rr-server activate
neighbor RD-BGP-SOURCE activate
neighbor v6-rr-server activate <==
neighbor 10.1.1.1 peer-group rr-server
neighbor 10.1.1.2 peer-group rr-server
neighbor 192.168.1.1 peer-group RD-BGP-SOURCE
no auto-summary
no synchronization
exit-address-family
```

Condition 2: This symptom is observed when the v6 peer-group is activated under the IPv4 address family as soon as it is created.

Workaround 2: There is no workaround.

- CSCek57749

  Symptoms: Execution of the **show version** or **show hardware** commands during traffic may result in packet drops.

  Conditions: This symptom occurs when executing the **show version** or **show hardware** commands.

  Workaround: There is no workaround.

  Further Problem description: Disabling NETIO interrupts/executing interrupt handlings of higher priority than NETIO interrupts have always been a source of packet drops on Cisco 7200 (as is the case with other uni-processor systems, for example CSCed10454). The drops usually occur due to lack of descriptors.

  The **show version** and its constituent functions make use functions which are implemented as exceptions, which are user generated exceptions of higher priority than any interrupts.

- CSCek75931

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

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

  Workaround: There is no workaround.

- CSCek78050

  Symptoms: Router console hangs.

  Conditions: The **dir bootflash:** command is entered after loading an onboard failure logging (OBFL) enabled image for the first time.

  Workaround: Reload the router to clear the issue.

- 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.

- CSCek79311

  Symptoms: Under stress conditions, an L2TP multihop node may crash.

  Conditions: This symptom is observed when a session is being disconnected.

  Workaround: There is no workaround.

- CSCsb36463

  Symptoms: IGMP packets are rate limited when they arrive on a layer 3 port (routed port) and are sent to the route processor.

  Conditions: The IGMP packets can be rate-limited if (1) IP-option rate limiter is configured using the **mls rate-limit multicast ip-options** *pps packets-in- burst* command, and IGMP packets contain router alert option. (2) FIB miss rate limiter is configured using the **mls rate-limit multicast ipv4 fib-miss** *pps packets-in- burst* command.

  Workaround: Configure ports as switchports with an SVI instead of a routed port or increase rate limiter parameters to allow expected level of IGMP packets.

- CSCsc77148

  Symptoms: Device may crash when the **show ipx cache** command is entered.

  Conditions: The **show ipx cache** command displays IPX cache entries. If there are a lot of entries, it will display few entries first and the remaining entries can be viewed by pressing space bar. If an entry is freed during this time (before we hit the space bar to view that entry), then it leads to accessing freed memory and hence crash.

  Workaround: There is no workaround.

- CSCse15434

  Symptoms: When running Inverse Multiplexing over ATM (IMA) on a router with shaping parameters configured under the **vc-class atm** global configuration command, the shaping parameters will be removed upon a reload of the router.

  Conditions: This symptom has been observed on a router with shaping parameters configured under the **vc-class atm** global configuration command for an IMA interface of PA-A3-8T1IMA/PA-A3-8E1 IMA PA.

  Workaround: Configure the native ATM shaping directly under the PVC instead of using a vc-class.

- 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.

- 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.

- CSCsg42672

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

  Conditions: Occurs with the following configuration sequence:

```
RR#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
RR(config)#router bgp 65001
RR(config-router)#neighbor rrs-client fall-over ?
  bfd        Use BFD to detect failure
  route-map  Route map for peer route
  <cr>

RR(config-router)#neighbor rrs-client fall-over

RR#sh ru
<snip>
router bgp 65001

 neighbor rrs-client peer-group
 neighbor rrs-client remote-as 20959
 neighbor rrs-client update-source Loopback0
 neighbor rrs-client fall-over route-map rrs-client <<<<<<<
```

  The route-map does not exist.

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

- CSCsg59059

  Symptoms: A device configured with Dynamic NAT (Network Address Translation) and Class B NAT pool may reload unexpectedly.

  Conditions: The symptom is observed when "ip nat pool" is configured with a prefix-length of 17, and when 32766 or more netflow entries pass through the device. If the nat pool is cleared by using the **clear ip nat translation** *, the device unexpectedly reloads.

  This does not affect Class C NAT pools and NAT Overload configurations.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsh33518

  Symptoms: When STP is configured on a Cisco Catalyst 6500 switch with Active and Standby SUP the **show spanning tree** command on the Standby SUP may show different information from that of Active SUP.

  For example:

```
Active SUP
   xs6k3#<CmdBold>sh spanning-tree <noCmdBold>

   VLAN0002
     Spanning tree enabled protocol ieee
     Root ID     Priority    32768
                 Address     0014.1bc4.c002
                 Cost        4
                 Port        259 (GigabitEthernet3/3)
                 Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

     Bridge ID   Priority    32768
                 Address     0014.1bc4.f802
                 Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
                 Aging Time 15

   Interface           Role Sts Cost      Prio.Nbr Type
   ------------------- ---- --- --------- -------- --------------------------
-
 ---
   Gi3/3               Root FWD 4         128.259  P2p
   Gi3/4               Altn BLK 4         128.260  P2p

   xs6k3#


   Spanning Tree info on Standby
   -----------------------------
   xs6k3-sdby#<CmdBold>sh spanning-tree <noCmdBold>
```

```
No spanning tree instance exists.


xs6k3-sdby#
```

Conditions: This condition is generic for Cisco IOS Release 12.2(18)SXF6 and earlier releases.

Trigger: This problem is due to the different load conditions on the Active and Standby SUP.

Impact: No spanning tree instance exists on standby.

Workaround: Manually reset Standby SUP to re-sync STP states from Active to Standby. However the STP states may digress again going forward.

Further Problem Description: This problem is due to the different load conditions on the Active and Standby SUP. Occasionally the Standby SUP may run ahead of Active SUP in terms of sync state. When there is a surge of activities on the Active SUP it may run behind the sync request/event coming from the Standby. When the sync event arrives too early the Active SUP drops the request due to wrong state/event combination and therefore the sync never happened and hence the discrepancy.

A fix is put in place to avoid this type of sync race condition between Active and Standby.

- 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.

- 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.

- 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/warp/public/707/confaccesslists.html

- 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.

- CSCsi32646

  Symptoms: The following message may appear on the console after a line card reset or OIR.

  ```
  %UTIL-3-IDTREE_TRACE: PW freelist DB:Duplicate ID free ...
  ```

  Conditions: This symptom is observed when xconnects are configured on the line card interfaces and multiple RP switchovers have been performed.

  Workaround: There is no workaround.

- CSCsi55626

  Symptoms: Packet buffer corruption may occur when report suppression is enabled and an MLDv2 report with multiple group records is received.

  Conditions: The symptoms are observed when MLD snooping is enabled. When one of the group records (join or leave) in the MLDv2 report is suppressed by MLD snooping, the problem will occur.

  Workaround: There is no workaround.

- CSCsi83287

  Symptoms: The following error message is displayed on the console:

  ```
  %ALIGN-3-SPURIOUS T/B ipv6fib_gre_ipv6_classified
  ```

  Conditions: This symptom occurs when an IPv6 tunnel transport endpoint receives fragmented IPv6 packets

  Workaround: Use a smaller tunnel MTU on the remote end of the tunnel to prevent fragmentation.

- CSCsi86339

  Symptoms: Packets incorrectly go out Traffic Engineering (TE)-Fast Reroute (FRR) back-up tunnel.

Conditions: This symptom occurs when FRR is enabled on a TE tunnel, when 7600-SIP-600 or 7600-ES20 are used as the MPLS facing line card for SVI based EoMPLS or VPLS. PFC-based EoMPLS is not affected.

Workaround: There is no workaround.

- CSCsi97434

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

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

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

- CSCsj00870

  Symptoms: BADSHARE error messages and traceback are seen during system bootup, switchover or online insertion and removal (OIR). Example:

  ```
  %SYS-DFC6-2-BADSHARE: Bad refcount in datagram_done, ptr=47AA3E2C, count=0
  Traceback= 401419BC 40141BDC 401906CC 40C9A2C8 40D2B08C 40D2BCFC 40D2C8A4 40D2D1F4
  4062992C 40629A40 406E370C 406E5ADC 40632F74 402AA848
  ```

  Conditions: Occurs in Cisco Catalyst 6000 series switches running various releases of Cisco IOS Release 12.2SR.

  Workaround: There is no workaround.

- 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.

- CSCsj56281

  Symptoms: Inherit peer-policy does not work after router reload.

  Workaround: There is no workaround.

- CSCsj67096

  Symptoms: Traffic comes in on a port-channel trunk on one VLAN, is routed via NAT on Supervisor Engine 720, and then sent back on same port-channel on another VLAN. Because the source index is not getting re-written after NAT, the traffic gets dropped.

  Note that if the traffic comes in on one port of the channel and goes back on the same port, the packets get rewritten correctly but are subjected to partial packet loss.

  Conditions: Occurs on the following configuration:

  - Cisco Catalyst 6000 series switches
  - Supervisor Engine 720

  - Cisco IOS Release 12.2(18)SXF7

  When the above has a port-channel configured with combination of non-fabric-enabled and fabric-enabled cards (such as WS-X6408 and WS-X6516) and this port-channel is configured as a trunk, the symptoms occur.

  Workaround: The workaround is to shut one member of the port-channel, so that traffic comes in on one port and is routed out on the same port on the switch.

  Alternatively you can use either fabric-enabled cards or non-fabric-enabled card in the port-channel. Avoid combining non-fabric-enabled and fabric-enabled cards.

- CSCsj85065

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

  Cisco has released free software updates that address this vulnerability.

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

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

- CSCsj87687

  Symptoms: A router may crash during startup when MPLS is configured.

  Conditions: The symptoms occur when starting up an MPLS IOU network with all the IOU instances starting with “-e” or “-s5”.

  Workaround: There is no workaround.

- CSCsj91123

  Symptoms: Router reloads after authentication attempt fails on console.

  Conditions: Occurs while performing AAA accounting. The accounting structure was freed twice, which results in crash. Occurs when the **aaa accounting send stop-record authentication failure** command is configured, which sends a stop record for authentication failure.

  Workaround: Remove the **aaa accounting send stop-record authentication failure** command.

- CSCsk05653

  Symptoms: The **aaa group server radius** subcommand **ip radius source-interface** will cause the standby to fail to sync.

```
c10k-6(config)#aaa group server radius RSIM
 c10k-6(config-sg-radius)#ip radius source-interface GigabitEthernet6/0/0


 c10k-6#hw-module standby-cpu reset
 c10k-6#
%REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_NOT_PRESENT)
%C10K_ALARM-6-INFO: ASSERT MAJOR RP A Secondary removed
%REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_DOWN)
%REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_REDUNDANCY_STATE_CHANGE)
%REDUNDANCY-3-STANDBY_LOST: Standby processor fault
```

```
(PEER_NOT_PRESENT)
%REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_DOWN)
%REDUNDANCY-3-IPC: cannot open standby port no such port
%RED-5-REDCHANGE: PRE B now Non-participant(0x1C11 =>
0x1421)
%REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a
standby insertion (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

%RED-5-REDCHANGE: PRE B now Standby(0x1421 => 0x1411)
%C10K_ALARM-6-INFO: CLEAR MAJOR RP A Secondary removed
-Traceback= 415C75D8 4019FB1C 40694770 4069475C
CONFIG SYNC: Images are same and incompatible

%ISSU-3-INCOMPATIBLE_PEER_UID: Image running on peer
uid (2) is the same
 -Traceback= 415CCC2C 415C75FC 4019FB1C 40694770 4069475C
Config Sync: Bulk-sync failure due to Servicing
Incompatibility. Please check full list of mismatched commands via:
   show issu config-sync failures mcl

Config Sync: Starting lines from MCL file:
 aaa group server radius RSIM
  ! <submode> "sg-radius"
 - ip radius source-interface GigabitEthernet6/0/0
```

Conditions: This symptom is observed if the **aaa group server radius** subcommand **ip radius source-interface** CLI is configured on a box with dual PREs.

Workaround: If the customer does not use the **aaa group server radius** subcommand **ip radius source-interface** *interface*, this will not be a problem.

If they use the **aaa group server radius** subcommand **ip radius source-interface** *interface* on a Cisco 10000 router in simplex mode (a single PRE), this will not be a problem.

If they run with dual PREs, then they will need to remove the **aaa group server radius** subcommand **ip radius source- interface** *interface* from the configuration as a workaround.

Removing the **aaa group server radius** subcommand **ip radius source-interface** *interface* from the configuration could cause problems for the customer. The radius server may be expecting the request to come from a specific source address. The router will now use the address of the interface the packet egresses the router from, which may change over time as routes fluctuate.

- 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.

- CSCsk19497

  Symptoms: Service-policy is removed from Multilink Frame Relay (MFR) interface.

  Conditions: Occurs during QoS stress testing while running the c10k3-p11-mz.122-32.8.86.SR image. The issue is triggered by performing a shut/no shut on the interface.

  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.

- CSCsk32095

  Symptoms: The Ethernet interface flaps after configuring QoS on the interface.

  Conditions: Occurs on PA-2FE-TX port adapter after applying QoS to the interface.

  Workaround: There is no workaround.

- CSCsk38024

  Symptoms: Etherchannel sync issues may be seen on the standby router. Some of the port-channel member ports might come up on the standby in an “unbundled” state, while on active they are in a bundled state.

  Conditions: The symptom occasionally occurs during router bootup of a High Availability system. The issue is seen when Fast Etherchannel configuration is present in the startup configuration.

  Workaround: There is no workaround.

- CSCsk40506

  Symptoms: An NSE-100 may crash when adding/removing mVPN configurations multiple times.

  Conditions: The symptom occurs when adding/removing mVPN configurations multiple times through two telnet consoles (one is for adding mVPN, the other for removing mVPN), while end-to-end traffic is on.

  Workaround: There is no complete workaround for this defect. If we avoid removing/adding mVPN configurations multiple times it may not occur.

- CSCsk41134

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

  – The RSA signature negotiation fails with a “signature invalid” message.
  – The certificate based authentication with ISAKMP profiles will not select the correct profile, and the connection will use the default settings.

  In all these cases the ISAKMP negotiations do not work.

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

  Workaround: There is no workaround.

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

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

  or possibly

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

In the second case you will either see:

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

Or

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

 (Notice the empty "Dist. name" field)
```

- CSCsk43058

  Symptoms: The interfaces on the Initial Wireless Services Module (WiSM) controllers are not pingable.

  Conditions: Occurs after upgrading a Supervisor Engine 720 to Cisco IOS Release 12.2(33)SXH. The first interface assigned to the port channel shows as being active in the port channel and the others show as suspended.

  Workaround: All interfaces will come up in the port channel and connectivity will be restored if the **mls qos** command is removed and then readded to the Supervisor Engine 720 global configuration.

- 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.

- CSCsk54061

  Symptoms: Memory allocation failed atm_vpivci_to_vc error occurs and device crashes.

  Conditions: Occurs while configuring for ATM-AutoVC or with incoming ATM traffic.

  Workaround: There is no workaround.

- CSCsk55423

  Symptoms: Cisco 7600 series router experiences flaps when processing Intermediate System-to-Intermediate System (IS-IS) traffic.

  Conditions: Occurs because Border Gateway Protocol (BGP) packets are placed in high-priority extended headroom. Such packets should placed in the plain headroom and not the extended headroom.

  Workaround: There is no workaround.

- CSCsk67466

  Symptoms: PVC may not come up on the ATM main interface.

  Conditions: The symptom is observed on a peer-to-peer (P2P) sub-interface that is configured for PVC.

  Workaround: There is no workaround.

  Further Problem Description: On a P2P sub-interface configured for PVC, allow the PVC to come up. Then delete the subinterface and recreate the same PVC on the main interface. The PVC does not come up (stays in INACTIVE mode). Spurious memory access may also be seen in this process.

- CSCsk68320

  Symptoms: A switch aborts or reloads after the **no ip routing** command is entered.

  Conditions: This symptom is observed when a Supervisor Engine IV is configured with a minimal IP multicast and Multicast Source Discovery Protocol (MSDP) configuration.

  Workaround: There is no workaround.

- CSCsk80552

  Symptoms: Delay seen in forming of Protocol Independent Multicast (PIM) auto-RP mapping. Whenever a link flaps, the graft messages are sent for faster convergence and since these get dropped over the multicast distribution tree (MDT) tunnel, there is a delay in convergence.

  Conditions: Occurs in networks with mVPN deployment and PIM-DM in the core. An interface flap on the PE/CE router may cause delay in forming PIM auto-RP mapping. The issue causes traffic black holing and affects the sources and receivers in the network, if the following conditions hold TRUE:

  a. If the network has a mVPN deployment, and the path between source and receiver has to traverse through the mVPN cloud.

  b. If traffic is processed by at least one Cisco 6500 or Cisco 7600 series router in the mVPN deployment. This occurs when Cisco 6500 and Cisco 7600 series routers are used to decapsulate traffic.

  Workaround: Migrate to PIM-SM. No functionality is affected and the fix for the same is available in Cisco IOS Release 12.2SXF.

  Further Problem Description: The PIM-DM graft messages, unlike other PIM-DM control packets, are unicast packets. These packets when sent over the MDT tunnel, are encapsulated with multicast MAC address and a unicast IP address (destination IP of the tunnel). Such packets are not replicated and are dropped.

- CSCsk83683

  Symptoms: After reload or switchover, when an initial request is made for a rsvd_vlan, VLAN allocation is not ready at that time.

Conditions: Occurs when route-map contains is configured with VPN routing/forwarding (VRF) on an interface. The issue creates a synchronization problem between Active & Standby, causing traffic to be punted to RP after reload or SSO.

Workaround: Remove the VRF and route-map, then apply it again to the interface.

- 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.

- CSCsk86642

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

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

  Workaround:

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

- 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.

- CSCsl02649

  Symptoms: PVC goes to INACTIVE state on standby after performing a **shut/no shut**.

  Conditions: Occurs when there are 4,000 active point-to-point access PVCs configured on a single port of a ATM-OC3 SPA of a Cisco 7600 series router. All of the PVCs have Routed Bridged Encapsulation (RBE) configured. All the PVCs are up initially on both active and standby console. If a **shut/no shut** is performed on the main interface, PVCs comes up on the active console but stays in inactive state on standby. The PVCs do not come up on standby even after line card online insertion and removal (OIR.

  Workaround: There is no workaround.

- CSCsl04764

  Symptoms: Crash when bringing up more than 2,000 DHCP class aware sessions.

  Conditions: This happens only for DHCP initiated sessions with class association, such as when “initiator dhcp class-aware” is configured. Memory corruption might occur when multiple DHCP sessions are being brought up. The corrupting pattern is the DHCP classname. The memory corruption occurs when the configured DHCP class name is offered after the DHCP workspace for the particular DHCP discover message has been cleared.

  Workaround: There is no workaround.

- CSCsl04835

  Symptoms: A route introduced by Conditional Route Injection is not removed from the iBGP peer upon withdrawal.

  Conditions: Consider this situation: Router B is a BGP router that has two eBGP peers, Router A and Router C. In a situation where RTR_A advertises a prefix and RTR_B injects a more specific prefix of it, the symptom is observed in two ways:

  1. If RTR_A withdraws the advertised prefix, the more specific prefix is removed on RTR_B, but this withdrawal is not sent to RTR_A and RTR_C.
  2. If the conditional route injection configuration is removed on RTR_B, the more specific prefix is removed on RTR_B, but this withdrawal is not sent to RTR_A and RTR_C.

  Workaround: There is no workaround.

- 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.

- CSCsl06110

  Symptoms: Port-channel interfaces are ignored when read from the DHCP snooping database

  Conditions: When the DHCP snooping database is read in, entries pointing to port channel interfaces are ignored.

  Workaround: There is no workaround.

Further Problem Description: This is a fairly uncommon case. The database is only read in on a full reload or if forced manually. In normal operation, port-channel interfaces can be used as DHCP snooping interfaces with no adverse effects.

- CSCsl06336

  Symptoms: When the **maximum-paths** *n* **import** command is unconfigured, for example, a **no maximum-paths** *n* **import** *m* command is issued for a VPN/VRF on a router, sometimes the routes in that VPN may have duplicate path entries.

  For example:

```
diezmil#sh ip bgp vpnv4 v v1001 10.0.20.0
BGP routing table entry for 100:1001:10.0.20.0/24, version 1342275
Paths: (2 available, best #1, table v1001)
Flag: 0x420
  Not advertised to any peer
  65164, imported path from 100:1:10.0.20.0/24
    192.168.1.7 (metric 4) from 192.168.1.254 (192.168.1.254)
      Origin IGP, metric 1552, localpref 80833, valid, internal, best
      Extended Community: RT:100:1001
      Originator: 192.168.1.7, Cluster list: 192.168.2.7
      mpls labels in/out nolabel/291
  65164, imported path from 100:1:10.0.20.0/24
    192.168.1.7 (metric 4) from 192.168.1.253 (192.168.1.253)
      Origin IGP, metric 1552, localpref 80833, valid, internal
      Extended Community: RT:100:1001
      Originator: 192.168.1.7, Cluster list: 192.168.2.7
      mpls labels in/out nolabel/291
```

  Workaround: The least resource-intensive workaround is to configure and unconfigure a dummy import map under that VPN/VRF. Clearing the affected BGP sessions on PEs also resolves the issue.

- CSCsl07297

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

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

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

- CSCsl09874

  Symptoms: OSPF may generate traceback when interface of router goes down or shut down administratively.

  Conditions: Affects Cisco IOS Release 12.4(15)T and later and Cisco IOS Release 12.2SRC.

  Workaround: There is no workaround.

- CSCsl10489

  Symptoms: Optimized Edge Routing (OER) feature may choose an exit with a lower Mean Opinion Score (MOS) when current exit has a better MOS. It does not consider the current exit when it selects the best exit based on MOS.

  Conditions: Occurs when MOS is configured as Priority 1 in the OER policy rules for a certain application.

  Workaround: There is no workaround.

- CSCsl11335

  Symptoms: The number of entries obtained from the “ciscoMvpnBgpMdtUpdateTable” table using the **getmany** command is incorrect

  Conditions: Occurred on a Cisco 7200 router running Cisco IOS version 12.4(17.9)T.

  Workaround: There is no workaround.

- CSCsl11743

  Symptoms: Multilinks are down after a switchover.

  Conditions: This symptom is observed when dMLP and RPR+ are configured on a Cisco 7500 router and a switchover occurs.

  Workaround: Micro-reload the Cisco 7500 router.

- CSCsl11868

  Symptoms: With IP Cisco Express Forwarding (CEF) enabled, ACL is not denying packets as intended in MPLS scenario. Alternate ping passes with IP CEF enabled through an ACL, even though ping should fail. When IP CEF is disabled, the ACL works as expected.

  Conditions: This is observed on router running Cisco IOS Release 12.4(17.9)T image with CEF enabled.

  Workaround: If possible, disable CEF using the **no ip cef** command. There is no workaround for the MPLS environment.

- CSCsl12827

  Symptoms: Transit IPSec packets are dropped in VPN routing/forwarding (VRF) mode.

  Conditions: Occurs when VRF is configured and a Catalyst 6500 series is a transit router for IPSec.

  Workaround: There is no workaround.

- CSCsl12836

  Symptoms: Logging voltage sensor values can cause excessive CPU usage. Sensor values are logged by On Board Failure Logging application, which is enabled by default.

  Conditions: Excessive CPU usage may happen in rare conditions when a card has more than 12 voltage sensors.

  Workaround: There is no workaround.

- CSCsl18765

  Symptoms: On a Catalyst 6500 or Cisco 7600, if a xconnect L3 Ethernet port is configured as source of a span session, it can cause the following issues:

  – Duplication of traffic on the VC

  – Packet reflected back on the VC leading to CE of the EoMPLS tunnel to disable its port for loopback or spanning-tree reason

  - Loop between ingress and egress PE.

  Conditions: This bug seen with following releases:

  - Cisco IOS Release 12.2(18)SXF7
  - Cisco IOS Release 12.2(33)SRA4
  - Cisco IOS Release 12.2(33)SRB2

  It may impact additional releases. Problem is not seen with PFC3C.

  Workaround: Do not span a xconnect port

  This is an hardware limitation. The fix of this defect is not fixing the faulty behavior. It is just present to disallow the user to use a xconnect port as a span source to avoid to accidentally hits this problem

- CSCsl19375

  Symptoms: A Cisco 7600 series router that is configured with VPLS under SVI, the state of the VPLS VCs may show as UP even when the SVI is down.

  Conditions: This behavior exists for VPLS in SR releases since SRA. The VPLS VCs are allowed to be provisioned and be UP as soon as the **no shutdown** command is applied. The interface VLAN reflects the state of the Ethernet switchports connected, and the VC state indicates if the VFI was provisioned. The VPLS VC circuit was able to come up.

  Workaround: There is no workaround.

- CSCsl20856

  Symptoms: The OSPF SNMP code may run for an extended period on systems with many interfaces. This can prevent other tasks in the system from being scheduled as quickly as they need to be.

  Conditions: Problem is seen when having large number (greater than 1000) interfaces on the router with OSPF configured on only a few (or none) of them and when running SNMP queries on OSPF MIB.

  Workaround: There is no workaround.

- CSCsl21668

  Symptoms: MPLS packets are punted to RP during tag2tag operation for the Scalable EoMPLS VCs. Scalable EoMPLS is the type of EoMPLS VC where the xconnect is configured on the EVC or on the subinterface of a SIP-400 line card.

  Conditions: Occurs when a shut/no shut is done on the core facing line card. Also occurs when online insertion and removal (OIR) is performed on the card.

  Workaround: Decrease the rate of punted packets to RP, which will reduce the CPU load to correct the problem.

  Further Problem Description: The tag2tag adjacency on the forwarding engine is programmed as punt, which causes packets to be punted to RP. The tag2tag adjacency is programmed as punt because the adjacency is incomplete during OIR or shut/no shut operation. Hence, if the traffic to the route processor is reduced adjacency could be completed by ARP.

- CSCsl23306

  Symptoms: The standby RP or standby SP may crash.

  Conditions: The symptoms are observed when the RP neighbor is adding or deleting CTS SXP (Cisco TrustSecure SGT Extended Protocol) connections, or attempting an SSO switchover with CTS SXP enabled.

  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.

- CSCsl27236

  Symptoms: WS-C6506-E with WS-SVC-IPSEC-1 keeps crashing with error %SYS-3-CPUHOG: Task is running for (126000)msec This is a CPU HOG SW forced crash.

  Conditions: The symptoms can be observed under stress conditions and when ipsec-isakmp is enabled.

  Workaround: There is no workaround.

  Further information: This is a day one bug that just surfaced. The customer found this under heavy stress conditions. The node list is getting corrupted, hence will iterate through the list indefinitely causing the CPU hog.

- CSCsl27984

  Symptoms: POS interface did not come up after the bootup of a Cisco 7600 router.

  Conditions: Issue was seen immediately after the bootup of Cisco 7600 router with POS interface module.

  Workaround: Problem was sorted out by removing and attaching the cable and then resetting the POS interface. After this procedure, POS interface came up and works fine.

- CSCsl28278

  Symptoms: Routes and packets are lost.

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

  Workaround: There is no workaround.

- CSCsl30331

  Symptoms: Prefixes are allowed by the outbound route-map even though the match condition is met and the action is set to deny.

  Conditions: Occurs in the following scenario:

  1. The iteration with the deny action contains a match community.
  2. The continue statement is used in one of the previous iterations.

  Workaround: If there is single match clause based on NLRI, the condition is avoided.

  Further Problem Description: Route-maps can be used without continue to avoid the problem.

- CSCsl31683

  Symptoms: PC error messages are seen along with tracebacks and SPA console is not available while running atlas BERT.

  Conditions: The issue is seen when running atlas BERT on CHSTM1.

  Workaround: Reload the SPA

- CSCsl32344

  Symptoms: Ports on WS-X6708-10GE or VS-S720-10G are disabled due to UDLD after supervisor failover. Flapping the port results in UDLD disabling the port again. Resetting the line card causes the ports to come online again.

  Conditions: Failover is the trigger for this issue to occur.

  Workaround: Reset the line card.

- CSCsl34523

  Symptoms: After an SSO mode switchover with PPPoX sessions the new active engine may display the following error message for one or more Virtual-Access interfaces:

  ```
  %COMMON_FIB-3-FIBIDBINCONS2: An internal software error occurred. Virtual-Access1.1
  linked to wrong idb Virtual-Access1.1.
  ```

  Conditions: The symptom occurs on the active engine after an SSO switchover when PPPoX sessions were active on the previously active engine.

  Workaround: There is no workaround.

  Further Problem Description: This error is not unique to any particular type of broadband PPP session.

- CSCsl38029

  Symptoms: After several thousand virtual private dial-up network (VPDN) sessions are created and torn down successfully, the router cannot create any new sessions. Either the L2TP Access Concentrator (LAC) or the L2TP Network Server (LNS) may fail with error message “VPDN Failed to obtain session handle.” This error message will be seen only when you enable the **debug l2tp errorr** command.

  Conditions: The maximum number of successful sessions before failure varies by platform.

  Workaround: Reload the router.

- CSCsl41230

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

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

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

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

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

- CSCsl41325

  Symptoms: A router crashes when BGP adjacency goes down. Lots of spurious memory access is seen.

Conditions: This symptom is observed on a Cisco 7600 series router with Supervisor 720-3BXL that is running Cisco IOS Release 12.2(33)SRB2. Multicast routing must be enabled and there must be multiple BGP paths with different preferences to a default route. If the preferred default route goes down this crash may be seen.

Workaround: Have only a single path to the default route.

- CSCsl41453

  Symptoms: When online insertion and removal (OIR) is performed with traffic flowing, the Multilink Frame Relay (MFR) interfaces will flap, and later the router will crash due to memory corruption.

  Conditions: The bug is seen only with scaled configs and OIR has to be performed while the traffic is being processed.

  Workaround: There is no workaround.

- CSCsl44109

  Symptoms: The number of physical queues is not equal the number of member links in a PC.

  Conditions: When QoS is configured on a PC interface, each member link gets a corresponding physical queue. Because of wrong algorithm for deletion of such queues, when member links flap, physical queues are deleted.

  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.

- CSCsl47374

  Symptoms: Calls per Second (CPS) was calculated with Standalone LNS and LAC for Cisco IOS Release 12.2SR. The CPS result obtained was compared with CPS results for SB4, XN3 and XD9 images and showed that there was a drop in CPS for Cisco IOS Release 12.2SR.

  Conditions: The symptom is observed when 8000 PPPOX/8000 L2TP sessions were brought up with a single local name configured under VPDN group configuration on LAC Router. It is also observed when 8000 L2TP Tunnels were brought up using different values in Tunnel-Assignment-Id in Radius Profile.

  Workaround: If different local names are configured under VPDN group configuration, the CPS drop will not be observed.

- CSCsl50569

  Symptoms: A SIP-400 module may drop all ingress packets destined for another fabric-enabled module. Prior to this, the module would be operating correctly.

  Conditions: This problem has only been seen with Cisco IOS Release 12.2(33) SRB2. The exact trigger is still unknown.

  Recovery: To recover connectivity, there are two options. Option 1 is preferable since it causes less traffic interruption. If Option 1 does not work, then Option 2 should be performed.

  1. Attach to the switch processor (**remote login switch**) and issue the command: **test fpoe index 0 FFFF restore**
  2. Reload the ingress SIP-400 line card: **hw-module module** *mod* **reset**

Workaround: To prevent issue from occurring in Cisco IOS Release 12.2(33)SRB2, diagnostics can be disabled on the SIP-400 with the following command:

```
Router(config)#no diagnostic monitor module "slot#" test 1
```

- CSCsl51607

  Symptoms: A router is not able to ping the second hop through the serial link that is configured with multilink virtual-template and encap ppp, although it can ping the next hop. Packets directed to other router through static route via virtual-access are getting dropped.

  Conditions: This symptom is seen in the Cisco IOS Release 12.2SR images c7200-ipbase-mz.autobahn76_111707 and c7200-ipbase-mz.122-32.8.99.SR.

  Workaround: There is no workaround.

- CSCsl51956

  Symptoms: Active supervisor may reload and fail-over to the standby supervisor while trying to reset Service and Application Module for IP (SAMI) in that chassis.

  Conditions: This happens only when SAMI line card is reset while upgrading the line card image. This crash will not happen if you reset the module after the upgrade is complete.

  Workaround: Always reset the SAMI LC after the completing the upgrade.

- CSCsl52092

  Symptoms: Port channel interfaces in the DHCP snooping database are not read back correctly when the database is refreshed. Either the interface is not recognized and the entry is ignored, or the entry may be assigned to the correct or an incorrect port channel.

  Conditions: Happens in any case when a port channel interface is found in a DHCP snooping database, and the database is read in.

  Workaround: Use an interface other than port-channel, or do not use the DHCP snooping database.

- CSCsl52220

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

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

  Workaround: There is no workaround.

- CSCsl53110

  Symptoms: A Standby RP may crash during SNMP bulk synchronization with errors in Community MIB.

  Conditions: The symptoms occur in a corner case. They may be seen during SNMP bulk synchronization of Community MIB, having communities with ACLs. Community entry, while being synchronized, is still pointing to deleted ACLs which leads to the Standby RP crashing at the time of bulk synchronization.

  Workaround: There is no workaround.

  Further Problem Description: This is a rare scenario which is applicable in VS setup with NAM card present.

- CSCsl53494

  Symptoms: The error messages generated for the SSC-400 card display incorrect product name.

  Conditions: Occurs in log messages. Product is incorrectly referred to as SSC-600 rather than SSC-400.

Workaround: There is no workaround.

- CSCsl55521

  Symptoms: Router may experience BGP convergence issues.

  Conditions: This problem has been seen when a lot of aggregates are configured on a router.

  Workaround: Add all aggregates after router has fully converged.

- CSCsl56547

  Symptoms: While getting the output of the **show mls cef ipv6 vrf** *id* for a valid VPN routing/forwarding (VRF), the following error message is seen:

  ```
  % vrf v6 doesn't exist.
  ```

  Conditions: This issue is seen only for IPv6 VRF. If both IPv4 and IPv6 are configured, then this problem does not occur.

  Workaround: There are two scenarios to reproduce this problem: 1 Configure VRF, save the configuration and reload the router. To workaround, configure the global **vtp mode transparent** command. 2 Configure VRF and toggle IPv6 unicast-routing. There is no workaround for this scenario.

  Further Problem Description: Doing a SSO switchover can also be used as workaround.

- CSCsl58473

  Symptoms: A router may crash due to a PXF DMA error.

  Conditions: The symptom is observed when Lawful Intercept (LI) and Ingress Netflow is configured on the interface.

  Workaround: There is no complete workaround. Disabling Ingress Netflow can help.

- CSCsl61164

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

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

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

- 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.

- CSCsl65327

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

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

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

- CSCsl65335

  Symptoms: A Catalyst 6500 or Cisco 7600 router running Web Cache Communication Protocol (WCCP) may reload when a WCCP redirect ACL is modified.

  Conditions: The router must be configured for WCCP L2 redirection with mask assignment and input redirection on one or more interfaces. Further, WCCP must be configured with a redirect ACL. The reload is triggered when the ACL is updated (modified) at the same time as an appliance is shutdown or fails.

  Workaround: If possible wait for the appliance to shutdown (WCCP-1-SERVICELOST) before updating the ACL.

  Further Problem Description: The reload may be more apparent when the WCCP control protocol is experiencing some instability - numerous WCCP-1-SERVICELOST, WCCP-5-SERVICEFOUND events - or if the appliance is being reconfigured at the same time as the ACL is updated.

- CSCsl66291

  Symptoms: In a Resilient Ethernet Protocol (REP) topology a hardware flood layer (HFL) packet is received on a node, but one of the REP interfaces is shut down.

  Conditions: REP needs to notify hardware flood layer (HFL) and anything over MPLS (AToM) clients about the VLAN list on the REP port along with the HFL notification, but in the above scenario it will send a list of all 4000 VLANS, causing non-REP related VLAN MAC addresses to be flushed as well.

  Workaround: There is no workaround.

- CSCsl68034

  Symptoms: Traffic might fail on Distributed Multilink PPP (dMLP) bundles when the SPA online insertion and removal (OIR) is done.

  Conditions: Occurs when a OIR is performed on a SPA with SIP-200 and Cisco 7600 router configured for dMLP bundles with member links from a SPA.

  Workaround: OIR of the SIP-200 line card will bring back the traffic up.

- CSCsl69206

  Symptoms: Ping does not pass through GRE tunnel which is a VPN routing/forwarding (VRF) member after second stateful switchover.

  Conditions: This occurs after a stateful switchover has happened twice on the router.

  Workaround: Reload the router.

- CSCsl70148

  Symptoms: On bootup with the 200 multicast-enabled, point-to-point, crypto GRE configuration, the tunnels are not installed in hardware and the entries are continuously deleted and recreated.

  Conditions: No explicit commands are run. This happens when booted with the above configuration and Cisco IOS Release 12.2(SX)F12.

  Workaround: There is no workaround.

- CSCsl70729

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

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

Workaround: There is no workaround.

- CSCsl72281

  Symptoms: After a Cisco 7600 series router reloads, host routes created by DHCP relay process for DHCP clients that are connected to unnumbered VLAN interfaces point to wrong VLAN interface.

  Conditions: This symptom occurs when interface-index value parameter on the router changes after the router reloads. This parameter is stored in DHCP bindings database on TFTP or FTP server. It is recalculated in case of the router reloading and may change if a new interface is added or existing interface is removed from the configuration. For example, a single interface VLAN is added to the configuration prior to the router reloading.

  Workaround: There is no workaround.

- CSCsl72285

  Symptoms: MLP bundle may fail to come up when a queuing policy is applied under the VT.

  Conditions: The symptom is observed on a Cisco 10000 series router where a queuing policy is applied under the VT in an LNS.

  Workaround: Bring up the MLP bundle and then apply the queuing policy under the VT in an LNS.

- CSCsl72774

  Symptoms: A router may run out of memory and fail malloc due to a memory leak.

  Conditions: This problem only occurs on distributed platforms (like the Cisco 7600/Catalyst 6500) when the CEF consistency checkers have been enabled. By default, the CEF consistency checkers are disabled. When the CEF consistency checkers are turned on, memory is leaked on the RP, SP and line cards.

  If you want to use the consistency checkers, then do so for only short periods of time. For example, use the consistency checkers while diagnosing network problems.

  Workaround: Disable the CEF consistency checkers by using the following commands:

  ```
  no cef table consistency-check ipv4
  no cef table consistency-check ipv6
  ```

- 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.

- CSCsl76647

  Symptoms: The **clear crypto isakmp** command deletes SA with connection ID from 0 to 32766. The SA created with the VPN SPA has a connection ID higher than 32766, and cannot be singularly deleted.

  Conditions: This symptom occurs when SA is established using the VPN SPA.

  Workaround: There is no workaround.

- 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.

- CSCsl78582

  Symptoms: After performing stateful switchover (SSO) on a router, error messages followed by tracebacks are observed on Active RP.

  Conditions: Router is configured with Virtual Private LAN Services (VPLS) and SwEoMPLS VCs with multiple core-facing interfaces.

  Workaround: There is no functionality degradation.

- CSCsl79141

  Symptoms: The new Any Transport over MPLS VCs configured after their line card reset may not come up.

  Conditions: This occurs if those VCs are one-side configured on the remote when the line card resets.

  Workaround: Reconfigure the VCs on both sides to clear the problem.

- CSCsl79219

  Symptoms: Bidir shadow entries may not be installed in hardware thus blocking the multicast traffic in some conditions.

  Conditions: This symptom occurs on the Cisco Catalyst 6500 switch that is running with MVPN configuration. The core network is in PIM-Bidir mode and sometimes the “z” flag setting for data MDT groups is not populated to hardware.

  Workaround: Use the **clear ip mr** *mdt_group* command to solve the problem.

- CSCsl81011

  Symptoms: Hierarchical queueing framework (HQF) not cleared even after removing the service policy from the interface.

  Conditions: HQF hierarchy not cleared after entering the **no service-policy out** *pname* command. This is seen with Optical Services Module (OSM).

  Workaround: There is no workaround.

- CSCsl83211

  Symptoms: Some supervisor 32 cards running modular IOS software crash (silently) during bootup after a power cycle.

  Conditions: Occurs on Supervisor 32 running modular IOS following a power cycle.

  Workaround: Use a Cisco IOS image. Do not cold boot the turn of the power. Instead use the **reload** command.

- CSCsl83415

  Symptoms: After executing the following CLI commands (steps mentioned alphabetically) via a script (not reproducible manually), the router sometimes crashes:

  ```
  Test10 :
  ---------
  ```

```
a. clear ip bgp 10.0.101.46 ipv4 multicast out
b. clear ip bgp 10.0.101.47 ipv4 multicast out

Test 1:
--------
c. show ip bgp ipv4 multicast nei 10.0.101.2
d. show ip bgp ipv4 multicast [<prefix>]
e. config terminal
```

The crash does not happen for each of the following cases:

1. If the same CLI is cut-paste manually, there is no crash.
2. If the **clear cli** command is not executed, there is no crash.
3. If the **config terminal** command is not entered, there is no crash.

Conditions: The symptom occurs after executing the above CLI.

Workaround: There is no workaround.

- CSCsl85041

  Symptoms: Health monitoring tests will not trigger Call-Home message even when the threshold is reached.

  Conditions: When there is a hardware or software failure, health monitoring tests which run in the background may fail continuously. When the failure threshold is reached, a Call-Home message is expected but it will not be triggered without this fix.

  Workaround: There is no workaround.

- CSCsl85391

  Symptoms: When an interface comes up or when its IP address has changed, there is a race condition between the MPLS TE and OSPF code recognizing the event. As a result, when TE calls OSPF to build an opaque LSA containing the newly available link, OSPF may not be able to match the IP address with an interface number. This causes the link in question to be omitted from the opaque LSA.

  Conditions: The issue is found to be in the interface between TE and OSPF area.

  Workaround: Use **shut/no shut** to clear the problem.

- CSCsl86633

  Symptoms: SCHED-2-EDISMSCRIT: Critical/high priority process rf_cc_clear_counter_process may not dismiss message seen on supervisor switchover with SSO operating mode.

  Conditions: This message can be seen if port-channel configuration exists on the Cisco 7600. There is no known impact because of this message.

  Workaround: There is no workaround.

- CSCsl88931

  Symptoms: When a SPA-SER-4XT is being used, the following error message is seen:

  %SERIAL_12IN1-3-SPI4_HW_ERR: SPA 4/3: Port0 SNK SPI4 DIP4 Error was encountered.

  Conditions: A SPA-SER-4XT should be present in a MCP platform to hit this problem.

  Workaround: There is no workaround.

  Further Problem Description: Apart from the above error message the SPA functions normally and packet continue to pass through

- CSCsl89176

  Symptoms: Router crashes while polling for VLAN information.

  Conditions: This happens in all platforms where the device is polling for vlan information using vlanTrunkPortEntry via SNMP.

  Workaround: Configure the following commands:

  ```
  snmp-server view viewname 1 included
  snmp-server view viewname 1.3.6.1.4.1.9.9.46.1.6.1.1 excluded
  snmp-server community communitystring view viewname RO acl- num
  access-list acl-num permit snmp manager source address
  ```

  Note that the ACL is optional

- CSCsl89425

  Symptoms: Bidirectional Forwarding Detection (BFD) sessions do not scale. This symptom is especially visible with an OSPF client when one of the peers is rebooted after configuring the maximum number of BFD sessions.

  Conditions: This symptom occurs when configuring maximum BFD sessions or total number of BFD sessions too close to the maximum limit.

  Workaround: Configure 90 percent of the maximum allowed BFD sessions.

- CSCsl90265

  Symptoms: Class-Based Tunnel Selection (CBTS) member tunnels are not recovered while performing an SSO operation.

  Conditions: Occurs when CBTS is configured and a SSO is triggered The member tunnels are resignalled after the SSO recovery period, but this problem results in traffic loss while the recovery is in progress.

  Workaround: There is no workaround.

- CSCsl90341

  Symptoms: A Cisco 7600 series router that is running Cisco IOS Release 12.2(33) SRB2 does not report all the Netflow flows even though **ip flow ingress** is configured. This happens when the box comes up after reload. Also very few flows are exported to the collector.

  Conditions: This symptom occurs under the following conditions: - Interface NDE is configured in the box - After the 7600 has come up after the reload. - Box has to have SIP-400 LCs.

  Workaround: Configure **ip route-cache flow** on the main interface or configure **no ip flow ingress** followed by **ip flow ingress** on the sub-interface.

- CSCsl91038

  Symptoms: OIF are not correctly programmed.

  Conditions: The replication mode is egress. Multicast flows are injected from multiple ports and joins are received from the ports.

  Workaround: Use ingress replication mode.

- 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.

- CSCsl93629

  Symptoms: FlexWAN line card crashes on a Cisco 7600 router running Cisco IOS Release 12.2SR image.

  Conditions: Occurs when random-detect is enabled directly on an ATM main interface PVC and a policy- map is attached to the interface.

  Workaround: There is no workaround.

- CSCsl94059

  Symptoms: Traffic may fail to go through an EzVPN client and a server.

  Conditions: The symptoms are observed on a router that is acting as an EzVPN client.

  Workaround: There is no workaround.

- CSCsl94621

  Symptoms: For the ATM multi-VLAN to VC feature, when the remote end of the link flaps, the spanning tree instance for the VLAN gets lost, and traffic is no longer forwarded.

  Conditions: Occurs when the ATM VC is the only instance of that VLAN in the router.

  Workaround: If there is at least one other port on the same VLAN, spanning-tree remains, and there is no impact. Configure a switchport and allow all VLANs that are in the ATM multi-vlan VC.

- CSCsl94785

  Symptoms: If multiple interfaces on a line card are configured for REP segments, on reload some of the interfaces configured for REP segments may be lost.

  Conditions: The symptom is observed when multiple interfaces on a line card are configured for REP segments.

  Workaround: Reconfigure the REP segments on those interfaces.

- CSCsl95249

  Symptoms: Device crashes after performing a sequence of steps that is not typical in customer environments.

  Conditions: The issue would require many steps such as **no atm sub if**; reconfiguring it; attaching a policy-map to atm main interface twice and then an online insertion and removal (OIR) operation.

  Workaround: There is no workaround.

- CSCsl95664

  Symptoms: In a Cisco 7600 series router with hundreds of l2 VCs and l3 VRFs configured, after a reload, traffic to the l3 VPN prefixes having aggregate labelS might experience 10-20 minutes of failure before recovering.

  Conditions: This happens only in scaled configurations with hundreds of VRFs and L2 VCs with QoS enabled.

  Workaround: There is no workaround.

  Further Problem Description: After PE reload, all L3VPN traffic destined for aggregate labels takes a long time (20 minutes +) to recover. There seems to be a significant delay in getting the forwarding entries programmed in HW for aggregate labels.

- CSCsl97898

  Symptoms: A router may crash when the port-channel interface is shutdown.

Conditions: The symptom is observed in a scaled setup, when the port-channel interface is shutdown on a scaled setup with IPv6 multicast traffic and when the system is operating in egress replication mode.

Workaround: There is no workaround.

- CSCsl98498

  Symptoms: Tunnel interface is not coming up with the **tunnel mode ipip decapsulate-any** command enabled on the interface. Hence the tunnel will not pass any traffic.

  Conditions: This is seen when the **decapsulate any** option is configured with the **tunnel mode ipip** command.

  Workaround: There is no workaround.

- CSCsm01334

  Symptoms: Following message seen while booting up device. Sometimes this message appears for 2-3 minutes.

  ```
  "%failed to configure the mapping. make sure community already exists."
  ```

  Conditions: This message seen on standby supervisor when booted with Cisco IOS Release 12.2(32.8.11)XID112 image.

  Workaround: There is no workaround.

- CSCsm01399

  Symptoms: After a bus idle event on a module, it is expected for the first healthy interface to be shut down as part of the recovery process. On a 67xx 10G module, this interface may remain down and not recover to the original up state after the bus idle recovery routine is finished. The opposite side of that connection may remain up after the event.

  Conditions: Issue only observed after a bus stall on the affected module and only affects the first healthy port on the module. Issue has been observed in Cisco IOS Release 12.2(18)SXF12.

  Workaround: Avoid using the first port on the 10GE module, this port can remain administratively down. The first port on the module should be healthy and had passed online diagnostics. Alternatively, restore connectivity after the issue occurs by performing a **shut/'no shut** on the affected interface.

  This issue has been fixed in Cisco IOS Release 12.2(18)SXF13, Cisco IOS Release 12.2(33)SXH2, Cisco IOS Release 12.2(33)SRB3 or later releases.

- 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.

- CSCsm05646

  Symptoms: After an SSO switchover, an Interface VLAN (SVI) may remain in a DOWN state, although the VPLS VC state is UP. Bridged traffic is not affected, although L3 related traffic will be affected in the case of Routed EoMPLS/VPLS.

  Conditions: The symptom is observed on a Cisco 7600 series router that is configured with H-VPLS with MPLS access (Hierarchical VPLS with MPLS access), Routed EoMPLS or Routed VPLS, and operating in SSO Redundancy Mode, without a switchport or Multipoint Bridging EVC in the VLAN.

Workaround: The workaround is to add a switchport allowing the VLAN. This should keep the Interface VLAN in an UP state across the SSO switchover. Alternatively, a shutdown followed by a no shutdown in the Interface VLAN under the conditions above recovers the failure. This shutdown/no shutdown can be automated by using Embedded Event Manager, monitoring the SSO switchover and automatically issuing the shutdown/no shutdown on the Interface VLAN in question.

- CSCsm06740

  Symptoms: A memory leak occurs when CLI commands are issued when AAA command accounting is configured.

  Conditions: This issue occurs only when AAA accounting is configured. For example:

```
aaa accounting update newinfo
 aaa accounting exec default start-stop group GROUPINFO
 aaa accounting commands 15 default start-stop group GROUPINFO
```

  Workaround: Remove AAA accounting configuration.

- CSCsm06762

  Symptoms: When displaying routes in a routing table, the last update time may sometimes be shown as “7w0d” when the route has recently been updated. For example:

```
router#show ip route 192.168.116.152

Routing entry for 192.168.116.152/30
  Known via "rip", distance 120, metric 1
  Redistributing via bgp 6747, rip
  Advertised by bgp 6747
  Last update from 192.168.117.154 on GigabitEthernet2/5.2583, 7w0d ago
  Routing Descriptor Blocks:
  * 192.168.117.154, from 192.168.117.154, 7w0d ago, via
GigabitEthernet2/5.2583
      Route metric is 1, traffic share count is 1
```

  The following traceback may also be seen:

```
ROUTER: %IPRT-3-NDB_STATE_ERROR: NDB state error (BAD
EVENT STATE) (0x00)
192.168.116.152/30, state 7, event 2->1, nh_type 1 flags 4 -Process= "RIP
Router", ipl= 0,
pid= 494
```

  The updated route will no longer be visible in the forwarding plane.

  Conditions: In cases where a distance vector protocol is being used (e.g. RIP) and the route goes into holddown state and then comes out of holddown before the flushtimer has expired, the traceback described above may occur.

  Workaround: The route can be restored by doing:

```
clear ip route 192.168.116.152
```

- CSCsm09338

  Symptoms: The following tracebacks are sometimes seen on a switchover of a Cisco 7600 router:

```
%C6K_PROCMIB-DFC7-3-IPC_PORTOPEN_FAIL: Failed to open port while
connecting to process statistics: error code = no such port
```

Conditions: Occurs when at least one LAN line card is present in the chassis.

Workaround: There is no workaround.

- CSCsm09618

  Symptoms: When performing an ISSU upgrade between the Cisco IOS Release 12.2SRB and Cisco IOS Release 12.2SRC images, the SIP-400 and ES20 line cards may fail to come online.

  Conditions: The problem occurs when **issu runversion** is run on the active supervisor after **issue loadversion** has completed. Some line cards may fail to come online after the new supervisor comes online.

  Workaround: When the supervisor reaches terminal state for SSO, the user can configure **power enable module <x>** to re-enable the line card.

- CSCsm10103

  Symptoms: Attempting to modify queue parameters on a policy map under a port channel interface may result in changes to the primary member links only. The secondary member links retain the original values.

  Conditions: The symptoms are observed in a port channel interface with two or more member links and where EVCs are added under the port channel interface. Attempting to change the QOS parameters under the policy map will result in changes to the primary member link only.

  Workaround: Enter the **shutdown** command followed by the **no shutdown** command on the PC interface and problem is corrected.

- CSCsm12247

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

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

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

  Additional Information: The changes address also situation where some wccp clients are sending modified weight field in the wccp message and this way create a topology change situation.

  Additional Information: The changes address also situation where some wccp clients are sending modified weight field in the wccp message and this way create a topology change situation.

- 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.

- CSCsm12692

  Symptoms: IPv6 traffic is limited due to the rate-limiters when RP switchover occurs. The **show mpls forwarding-table** command indicates the duplicate label entries for IPv6 at the same time. Finally, the limited IPv6 traffic and the duplicated label entries are restored about 10 minutes later.

  Conditions: Occurs when RP switchover occurs with IPv6 VPN over MPLS (6VPE) configuration.

Workaround: There is no workaround.

Further Problem Description: Additionally, IPv4 entries work fine, and IPv4 traffic is not limited due to RP switchover.

- 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.

- CSCsm13408

  Symptoms: DHCP renew packets are ignored after a switchover.

  Conditions: This is only present after a forced switchover from Active to Standby RP, and only for VPN routing/forwarding (VRF) ip-sessions.

  Workaround: Prevent switch over, or extend the DHCP lease time to 24 hours or more.

- 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.

- CSCsm15406

  Symptoms: Spurious memory access is observed when router boots up.

  Conditions: Occurs when Virtual Private LAN Services (VPLS) is configured. Observed in a setup with 4,000 VFIs and about 8,000 VCs.

  Workaround: There is no workaround.

- CSCsm15687

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

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

  Workaround: There is no workaround.

- CSCsm16309

  Symptoms: Crash in Bidirectional Forwarding Detection (BFD) subsystem may occur after last BFD session is removed.

  Conditions: Occurs after all BFD sessions are removed and the BFD finishes cleaning up data structures.

  Workaround: There is no workaround.

- CSCsm17213

  Symptoms: Packet loss/connectivity issues in a IPv4 VRF due to traffic being sent to the rate-limiter and the VLAN-RAM table not being installed correctly. This is seen on interfaces which had an IPv6 address configured on it before.

Conditions: - The VRF needs to be configured for 6vPE and IPv4. - The 6vPE needs to be removed from the VRF definition by the **no address-family ipv6**.

Workaround: **Shut/no shut** the VLAN interface.

- 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.

- CSCsm20599

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

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

  Workaround: After creating a PVC on a P2P subinterface, call “exit” or “end”.

- CSCsm20994

  Symptoms: Kron occurrences are not rescheduled properly when the clock is set near the end of a calendar year.

  Conditions: A kron occurrence is scheduled daily or hourly. The clock is reset near the end of the year such that the next occurrence of the kron policy would happen in the next year.

  Workaround: After clock reset, remove/restore kron occurrences to cause them to be scheduled properly.

- CSCsm21728

  Symptoms: A router crashes when CPU_MONITOR between RP and SP messages have not been heard for more than 150 seconds. This is happening with a congested condition that is running on internal EOBC.

  Conditions: This symptom occurs when there are control data burst and congestions at internal EOBC.

  Workaround: There is no workaround.

- CSCsm23160

  Symptoms: The standby RP may unexpectedly reload and issue the following traceback:

  ```
  %SCHED-2-SEMUNLOCK: rf task attempted to unlock semaphore owned by interrupt.
  ```

  Conditions: The symptom is observed under rare conditions, usually after the standby RP starts to synchronize with the active RP.

  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 syncing initial data to the standby RP before standby hot state is reached in SSO mode.

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

  Impact: This issue affects operations.

  Workaround: Reload the active PRE if this issue occurs.

- CSCsm26150

  Symptoms: Router crashes while configured for Circuit Emulation over Packet (CEoP) SPA.

  Conditions: Issue is reproducible through script run (one of every 3 to 4 times).

  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

- CSCsm27455

  Symptoms: SNMP query on "mempool mib" is returning only "cempMemBufferNotifyEnabled," and other MIB instances are not populated. Hence "cempMemBufferNotifyEnabled" is empty.

  Conditions: Occurs on Cisco 7200 and Cisco 7300 platforms with "advipservicesk9" images. The issue does not occur with "adventerprisek9" images.

  Workaround: No workaround available.

- CSCsm27565

  Symptoms: The following CPUHOG is observed on executing the **show ip route** *protocol* command:

  ```
  %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs (2/1),process
  = Exec.
  ```

  Conditions: There must be a large number of routes in the routing table (e.g. 300K+ BGP routes), most of which are owned by a protocol other than that which has been specified in the **show** command.

  Workaround: Do not use the *protocol* argument to filter the routes which are displayed. If necessary, display the console output after the fact.

- CSCsm27814

  Symptoms: The dot3 and dot3StatsTable tables are empty with ETHERLIKE-MIB.

  Conditions: This issue is only observed with the c7200p-advipservicesk9-mz image. The issue does not occur in the c7200p-adventerprisek9-mz image.

  Workaround: There is no workaround.

- CSCsm27958

  Symptoms: After upgrading a Cisco 7600 to Cisco IOS Release 12.2(33)SRC, SSO does not come up and router stays in RPR.

  Conditions: Occurs only if the **passive-interface default** command is configured under OSPF.

  Workaround: After upgrade, unconfigure and configure again the **passive-interface default**.

- CSCsm28791

  Symptoms: PFC-based EoMPLS does not have the correct disposition adjacency sometimes on the ESM20G, SIP-600 line card.

  Conditions: This symptom is due to a race condition on the control plane update.

  Workaround: There is no workaround.

  Further Problem Description: Make sure that the EoMPLS VC is a PFC-based EoMPLS (i.e. it is configured on the sub-interface or the main interface). Make sure that the disposition is done on the ESM20G and SIP-600 line card.

  Using the **show mpls l2transport vc** *vcid* **detail** command, get the local label. Get the PFC adjacency using the **show mls cef mpls** *label* command and the **show mls cef adjacency entry** *addr* command. If the MTU is programmed as 65535 and dindex is 0x14, then you are hitting this problem.

- 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.

- CSCsm32555

  Symptoms: On a Cisco 7600, connectivity from a MPLS VPN to a GRE peer might fail due to inconsistent VPN ID programming.

  Conditions: Occurs when you toggle the **[no] mls mpls tunnel-recir** command over a VRF-aware GRE tunnel.

  Workaround: There is no workaround.

- CSCsm33193

  Symptoms: BGP convergence for 1->2 and 2->1 does not improve even if **cef table ... convergence speed** is enabled.

  Conditions: Occurs when a combination of L3VPN and L2VPN are configured.

Workaround: There is no workaround.

Further Problem Description: There is an improvement in BGP convergence (at 2.5 seconds) if you reduce the IS-IS prefixes to 2K. Otherwise convergence time is around 5 seconds.

- CSCsm33925

  Symptoms: NetFlow will not collect statistics in the Cisco 7200 “advipservices” and “spservices” images.

  Conditions: Occurs during normal NetFlow usage. Can affect any platform supporting these images.

  Workaround: Switch to a different Cisco IOS release or image.

- CSCsm34361

  Symptoms: TCP ports may not show open as required during port scanning using NMAP.

  Conditions: This symptom is observed on a Cisco 7200 router.

  Workaround: There is no workaround.

- 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.

- CSCsm36500

  Symptoms: Tracebacks are seen. These tracebacks have no functional impact.

  Conditions: Occurs on after online insertion and removal (OIR) of the 5x1 GE SPA of the SIP-600 on which multiple subinterfaces with IPv6 address have been created. This is a cosmetic issue and has no functional impact. The issue will eventually correct itself.

  Workaround: There is no workaround.

- 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.

- CSCsm38142

  Symptoms: Potential memory leak on Cisco 7600 RP due to software defect in 12.2SRB.

  Conditions: Occurs in routers running Cisco IOS Release 12.2SRB. It is observed if any QoS policy (service-policy command) is configured on the router. It only impacts distributed platforms such as the Cisco 7600. Eventually the router could exhaust all available memory.

  Workaround: There is no workaround.

- 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.

- CSCsm40013

  Symptoms: A Cisco 7600 configured with TE tunnels and FRR protection might experience a line card crash.

  Conditions: This might happen when the TE tunnels are shut. It is difficult to recreate and is unlikely to occur again.

  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.

- CSCsm42758

  Symptoms: A CPUHOG warning is logged for the environment polling process for VTT devices.

  Conditions: Problem seen during VTT device reading. CPU hogs can affect L2 protocols and cause link flaps. This affects RSP720 router only.

  Workaround: You can disable VTT temperature monitor with the following series of commands:

  ```
  config terminal
  service internal
  exit
  enable
  remote command switch test env poll disable vtt 1 temp 0
  remote command switch test env poll disable vtt 2 temp 0
  remote command switch test env poll disable vtt 3 temp 0
  ```

- CSCsm43482

  Symptoms: The traffic on a VC may be dropped on ingress PE in Virtual Private LAN Services (VPLS) network.

  Conditions: Occurs when another VC goes down in a different VLAN. The VC is up on affected VC during this problem. This problem can be restored using **shut/no shut** in target SVI interface on PE.

  Workaround: There is no workaround.

- CSCsm43938

  Symptoms: Standby PRE might reset at bootup while trying to sync over large ARP tables from the primary to the standby PRE.

  Conditions: The issue has been seem with very large (12 MB) configurations and large ARP tables (16K entries). The issue is only seen when the standby is booting up to standby mode.

  Workaround: There is no workaround.

- CSCsm44720

  Symptoms: OSPF sham-link does not come up on the rsp720 supervisor.

  Conditions: This is only observed when the aggregate label is recirculated in hardware. When the aggregate label is in VPN-CAM this issue is not observed. The **show mpls platform vpn-vlan-mapping** command can be used to check whether the aggregate label is on VPN- CAM or not.

  Workaround: If QoS is configured, then remove the QoS.

  Further Problem Description: There is a chance that the RP will crash if the sham-link is configured with the aggregate label is recirculated. Hence, it is advisable to remove sham-link in that scenario.

- CSCsm44914

  Symptoms: Standby RP does not sync with active RP on Cisco Intelligent Services Gateway (ISG) web logon sessions. The subscriber is authenticated on the active RP but the standby RP shows unauthenticated.

  Conditions: Occurs on Cisco 7600 routers configured with ISG.

  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.

- CSCsm46290

  Symptoms: Weighted Random Early Detection (WRED) does not take effect on the remarked CoS (Class of Service) value.

  Conditions: If a policy-map marks the COS field in the packet and also does WRED on the traffic classified in the same class, then WRED does not take effect on the newly marked CoS value.

  Workaround: There is no workaround.

- CSCsm46903

  Symptoms: The following error messages occur:

  ```
  %SPA_OIR-3-SW_INIT_TIMEOUT: subslot <slot>/<bay>: SPA initialization not completed.
  %SPA_OIR-3-RECOVERY_RELOAD: subslot <slot>/<bay>: Attempting recovery by reloading
  SPA
  ```

  Conditions: Occurs in a heavily loaded system with 16,000 xconnects and around 200,000 BGP routes. When traffic running is being processed during online insertion and removal (OIR), the line card fails to come up displays the error messages.

  Workaround: Perform another OIR of the line card.

- CSCsm47544

  Symptoms: Software/SVI-based EoMPLS with VC type Ethernet VLAN does not work with the following core-facing line cards:

  - SIP200
  - Flexwan
  - Enhanced Flexwan

Conditions: Occurs when the cards above are configured for xconnect SVI-based VLAN interface with MPLS. If the pseudo-wire VC type negotiated with peer is type 4/Ether Vlan, packets are sent across pseudo-wire with DOT1q VLAN tag removed causing ping to fail between CEs.

Workaround: Use one of the following as core-facing line cards:

- SIP-400
- SIP-600
- ES20
- PWAN2

- CSCsm49214

  Symptoms: ESM20G line card crashes upon removal of parent input VLAN range class in Ethernet Over MPLS (EoMPLS) configuration.

  Conditions: Occurs when traffic is flowing, and the parent class that matches this traffic in VLAN-based EoMPLS setup with MIV policy is removed.

  Workaround: There is no workaround.

- CSCsm49865

  Symptoms: The following message is displayed continuously: SRB02:VDB [301] state invalid. Retrying the event

  Conditions: Can occur when an interface flaps.

  Workaround: There is no workaround.

- CSCsm50309

  Symptoms: Border router crashes due to heartbeat failure while configuring Optimized Edge Routing (OER).

  Conditions: Occurred while configuring OER in a border router. After the **master IP key- chain password** was entered, the master came up and enabled netflow aggregation export v9, the CPU hung, and the device crashed.

  Workaround: There is no workaround.

- CSCsm51333

  Symptoms: Incorrect classification occurs when a policy-map with MIV matching on an input VLAN and another class-map matching on multiple input VLANs where one of them match on the VLAN already present in the other class. The overlapping class matches the input VLAN for which a class-map is already exclusively defined.

  Conditions: The policy-map needs to have two classes where some of the match input VLANs should overlap. This policy-map is applied in output direction on the core facing interface on an Ethernet Over MPLS (EoMPLS) setup.

  Workaround: There is no workaround.

- CSCsm51729

  Symptoms: After a router has been running continuously for more than 7 weeks, the last update time for routes in the routing table will be shown as “7w0d” when the route has recently been updated. For example:

```
router#show ip route 192.168.116.152


Routing entry for 192.168.116.152/30
  Known via "rip", distance 120, metric 1
```

```
  Redistributing via bgp 6747, rip
  Advertised by bgp 6747
  Last update from 192.168.117.154 on GigabitEthernet2/5.2583, 7w0d ago
  Routing Descriptor Blocks:
  * 192.168.117.154, from 192.168.117.154, 7w0d ago, via
GigabitEthernet2/5.2583
      Route metric is 1, traffic share count is 1
```

The following traceback may also be seen:

```
ROUTER: %IPRT-3-NDB_STATE_ERROR: NDB state error (BAD
EVENT STATE) (0x00)
192.168.116.152/30, state 7, event 2->1, nh_type 1 flags 4 -Process= "RIP
Router", ipl= 0,
pid= 494
```

If the traceback is seen, the updated route will no longer be visible in the forwarding plane and will not be redistributed.

Conditions: The router must be running continuously for 7 weeks.

Conditions for the traceback to occur:

- Router must be running continuously for at least 7 weeks.
- A distance vector protocol is being used (e.g. RIP), and the route goes into holddown state and then comes out of holddown before the flushtimer has expired.

Workaround: In the event of traceback, the route can be restored by doing the following:

```
clear ip route 192.168.116.152
```

The clear will NOT correct the update time on the routes, which will still be seen as 7w0d. The latter condition can only be cleared by either:

1. Rebooting the router
2. If redundant RPs are present, reboot the Standby RP, achieve SSO state, and force a switchover.

Either technique will provide another 7 weeks before either of the problems might be encountered again.

- CSCsm51942

  Symptoms: Crash occurs usually during or after saving configuration with an exception CPU signal 10 at RP.

  Conditions: This crash seems related with using SNMP and has been seen on Cisco IOS Release 12.2(33)SRC.

  Workaround: There is no workaround.

- CSCsm53035

  Symptoms: A few PBHK translations of sessions do not get deleted after idle- timeout in scale scenario (number of session => 4000).

  Conditions: This symptom is seen in scale scenario, when PBHK traffic is present on 4000 or more sessions.

  Workaround: In this case, chunk_malloc() is failing to allocate memory for a message going from DP to CP. We replaced chunk_malloc() by managed_chunk_malloc (), which solves the issue.

- CSCsm53392

  Symptoms: Line card is power cycled because Forwarding Information Base (FIB) is disabled on the line card. When this happens the following error message is generated:

  ```
  %FIB-2-FIBDISABLE: Fatal error, slot 2/0 (2)
  %SNMP-5-MODULETRAP: Module 2 [Down] Trap
  %OIR-SP-3-PWRCYCLE: Card in module 2, is being power-cycled off (FIB disabled on the line card)
  ```

  Conditions: FIB can be disabled on a given line card because of various reasons such as a software error or due to platform transport error.

  Workaround: When FIB disable occurs, the only way to recover from the issue is to perform an OIR. After the changes made by this change request the line card will be automatically reloaded. If user wants to disable the automatic reload of the line card enter the **platform cef linecard fib-disable action none** command.

  Further Problem Description: If user has configured the **platform cef linecard fib-disable action none** command on the router and performs an ISSU upgrade or downgrade to an release where the command is not supported, then MCL errors will be observed. This will cause the ISSU operation to fail. User is advised to remove the above command while performing the ISSU operation.

- CSCsm53489

  Symptoms: Following recovery, all traffic for a VC is lost. All imposition Ethernet Over MPLS (EoMPLS) entries are missing on core-side SIP-400 line card. The traffic does not switch back to the primary TE- FRR tunnel on SIP-400 from backup tunnel on other line card.

  Conditions: The problem is seen in Cisco IOS Release 12.2(33)SRB3.

  Workaround: Togglle the primary tunnel. On the primary tunnel performing a **shut/no shut** switches the traffic back to the primary tunnel from the backup tunnel.

  Further Problem Description: For the TE-FRR scenario in which SIP-400 is the primary/protected core- side interface, and other line card is the backup FRR LC/interface; traffic for software EoMPLS and Virtual Private LAN Services (VPLS) is not restored following a failover and re-optimization. It appears that software EoMPLS/VPLS core-side imposition entries do not exist on the SIP-400 line-card after re- optimization.

- CSCsm54548

  Symptoms: IP prec to exp bit marking does not work.

  Conditions: This problem rarely occurs in most routers. If the line card is reset abruptly by SP after the router is reloaded, there is a possibility that it might occur.

  Workaround: Toggle the **mlq qos** off and on again if the problem occurs.

- CSCsm54873

  Symptoms: Embedded Event Manager (EEM) rules may not trigger properly when performing SIP OIR.

  Conditions: EEM policies that interact with the IOS CLI through the **command action** command and EEM TCL policies that use the CLI library may not interact properly when triggered. Incorrect sequencing with the IOS CLI may result when the policies are triggered resulting in the IOS CLI commands not being invoked.

  This problem exists on all shipped versions of IOS XE.

  Workaround: There is no workaround.

  Further Problem Description: This can impact customers that use the Embedded Event Manager with EEM applets or policies that interact with the CLI.

It was seen on the ASR platform and other platforms when “sched heapchecks process” was enabled. A timing issue can cause EEM action CLI commands to not coordinate with the IOS exec properly.

The SIP2 is probably related to the ASR platform. An OIR event is used to trigger the specific EEM policy. This should occur with any EEM type policy however.

SXF is not impacted by this bug.

- CSCsm56140

  Symptoms: In an MR-APS environment, sometimes “working” channel CHOC12 card may get stuck in Signal Degrade state, forcing it to become a low priority link.

  Conditions: This symptom may been seen after long periods of traffic combined with several hw-module slot resets on a Cisco 10000 series router that is running Cisco IOS Release 12.2(33)SB. It may also be seen when cable has been pulled and reinserted into the active/working CHOC12 card.

  Workaround: Working controller can be returned to a healthy state by doing one (or more) of the following:

  - power-cycling router
  - pulling/reinserting CHOC12 card
  - pulling/reinserting cable at the ONS end

- CSCsm57494

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

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

  Workaround: There is no workaround.

- 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.

- CSCsm58677

  Symptoms: Occasional malloc failures at FW/SIPx cards pointing to PROCMIB process.

  Conditions: These are seen under heavily loaded Ethernet Out of Band Channel (EOBC) conditions. No straightforward trigger observed.

  Workaround: There is no workaround.

- CSCsm59499

  Symptoms: TOOBIG error msgs being displayed on the console.

  Conditions: The problem is seen on a Cisco 7600 router running Cisco IOS Release 12.2(33)SRB image when ES20 line card is subjected to online insertion and removal (OIR).

  Workaround: There is no workaround.

- CSCsm60223

  Symptoms: Crash may occur with error massage in the log:

%SYS-6-STACKLOW: Stack for process Per-Second Jobs running low Breakpoint exception, CPU signal 23, PC = 0x42789538

Conditions: Occurs when “mpls pal” and Netflow are configured.

Workaround: There is no workaround.

- CSCsm61067

  Symptoms: Traffic is not forwarded on VPLS pseudowires.

  Conditions: This symptom is seen on a VPLS setup with IGMP snooping enabled on the vlan interface hosting the VFI VCs. If a very quick **shut** followed by a **no-shut** is performed, this condition occurs.

  Workaround: A **shut** followed by a **no-shu**t on the VLAN interface is required to resume traffic.

  Further Problem Description: IGMP snooping is broken with no joints received.

- 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** *no* under ATM interfaces

  Repeating Step 2 continuously will cause a crash.

  Workaround: There is no workaround.

- CSCsm62033

  Symptoms: L2TP session does not come up.

  Conditions: Occurs when a Cisco router marks the Call Serial Number AVP in the ICRP as mandatory. This causes a third-party router to reject it.

  Workaround: There is no workaround.

- 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.

- CSCsm62748

  Symptoms: Issue seen on ES20 Line cards with MPB configuration on Ethernet virtual connection (EVC), Traffic on bridge domain is flooded and may be sent out on incorrect EVCs instead of being dropped by the filtering code.

  Conditions: Issue seen with MPB configuration on EVC, and it generally may be seen with VLAN range encapsulation on the EVC.

  Workaround: There is no workaround.

- CSCsm64643

  Symptoms: IPv6 prefixes for passive-interface are not advertised by Intermediate System-to-Intermediate System (IS-IS) feature.

Conditions: The problem seen with RSP720 card and only when the **passive-interface loopback0** command is used under the IS-IS configuration. This configuration works properly with SUP720 but NOT with RSP720.

Workaround: There is no workaround.

- CSCsm65584

  Symptoms: System convergence delay with scaled config.

  Conditions: With extensive traffic on Ethernet Out of Band Channel (EOBC) bus, RSP720 dual supervisor setup experiences excessive collisions. These excessive collisions result in EoBC packet drop and thus resulting in IPC re-transmission. This retransmission affects the convergence time.

  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>
  ```

- CSCsm66228

  Symptoms: Line card crashes while booting up and displays the following error message: Hardware or Software error occurred on Subslot 0. Reason : Fugu: RXHSPITSTATOOF Automatic Error recovery initiated. No further intervention required.

  Conditions: Occurs because one of ESM20 ports should not have XFP.

  Workaround: Insert valid XFP in two ports slot on esm20.

- 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.

- CSCsm66774

  Symptoms: When a MIV policy-map is attached to the core facing interface in the output direction, then classification is incorrect.

  Conditions: Occurs when MIV policy-map is applied to core facing interface in output direction.

  Workaround: There is no workaround.

- CSCsm69368

  Symptoms: Memory allocation failures and WATERMARK messages are seen on console.

  Conditions: Occurs when Netflow Data Export (NDE) is enabled with Netflow TCAM overflown with flows on a DFC. RP CPU utilization is high.

  Workaround: The system is not supposed to scale for that many flows. Disable Netflow for immediate fix.

- CSCsm71240

  Symptoms: Standby unable to ping to Virtual IP address.

  Conditions: Occurs when HSRP groups are removed or changed. The active router is not replying to the standby router with Virtual IP address ARP, and the ARP table in standby shows Virtual IP arp as incomplete.

  Workaround: There is no workaround.

- CSCsm71592

  Symptoms: In an MPLS environment the imposition traffic does not recover and is dropped on this router itself. Disposition traffic is going through fine.

  Conditions: This problem was observed after SSO switchover. This problem was observed internally when 600 Scale EoMPLS VCs are configured on the ES20 card as the CE facing link. 600 TE tunnel head ends are configured on this box. Each EoM VC is mapped to a different TE tunnel using the AToM tunnel select feature. Bi-directional traffic is going through this setup. The drop is due to the ADJ incomplete. It did not clear when the next ADJ update was received.

  Workaround: There is no workaround.

- CSCsm72807

  Symptoms: The following message is seen:

  ```
  %DHCP_SNOOPING-3-DHCP_SNOOPING_INTERNAL_ERROR: DHCP Snooping internal
  error, Unknown dhcp message type packet should be already handled so they should not
  come here, they
  will be dropped.
  -Traceback= 405B938C 405B98D0 406125EC 41FE7E6C 41FE7D8C 41FE8940 41FE8A90
  ```

  For each such message that appears, a random packet may be corrupted.

  Conditions: This happens with DHCP snooping configured with SSO. This will only happen on the Cisco 7600, and will only happen under stressful conditions.

  Workaround: Use RPR+ instead of SSO

- CSCsm72987

  Symptoms: When polling the ENTITY MIB for the gigabit ports that are integrated in the RSP720, there is an issue with entPhysicalParentRelPos for those Gigabit ports. They are reporting the same value.

  Conditions: Occurs on Cisco 7600 routers with the RSP720 card and running Cisco IOS Release 12.2(33)SRC and Cisco IOS Release 12.2(33)SRB1.

Workaround: There is no workaround.

- 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
```

- CSCsm74961

  Symptoms: The standby RP cannot synchronize with the active RP subscriber session status. The active RP shows the session is TAL(MAC+Opt82) authenticated and up, but the standby RP shows no active sessions.

  Conditions: Cisco 7600 configured as follows:

  - Initiator: IPoQ/DHCP
  - IP Address Assignment: Radius class name, ISG-DHCP Relay
  - Authorization: TAL (MAC+Opt82)
  - Network Service: VRF Mapping
  - Accounting: Postpaid
  - QoS: Session MQC
  - Service/features: Security ACL, ARP Ping, Open Garden

  Workaround: There is no workaround.

- CSCsm75286

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

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

  Workaround: Apply a fresh route-map.

- CSCsm75642

  Symptoms: Ping does not pass through GRE tunnel which is a VRF member after second SSO switchover.

Conditions: This occurs after a stateful switchover has happened twice on the router.

Workaround: Reload the router.

- CSCsm77171

  Symptoms: Router will crash.

  Conditions: Occurs with high traffic conditions where NetFlow has no free flows and multicast egress NetFlow is configured.

  Workaround: Disable multicast egress NetFlow.

- CSCsm77173

  Symptoms: Traffic stops after a policy with marking in user defined classes queueing in class-DFLT is applied to a sub-interface.

  Conditions: Occurs when the above type of policy is applied.

  Workaround: Perform a **shut** followed by a **no shut** of the sub-interface, then perform a false update of the policy map. For example, set the "class" parameter to the same value in the policy map.

- CSCsm79148

  Symptoms: SNMPwalk fails with packet too big error on enterprises.9.9.492 in the OID tree.

  Conditions: SNMPwalk failing with packet too big error.

  Workaround: Exclude the cermScalarsGlobalPolicyName SNMP object using a view as shown below:

  ```
  snmp-server view testview internet included
  snmp-server view testview cermScalarsGlobalPolicyName excluded
  snmp-server community public view testview RO
  ```

- CSCsm79995

  Symptoms: Spurious memory access may occur at line card which cause SIP-400 to crash.

  Conditions: May occur when attaching a service policy to any interface or removing the service policy.

  Workaround: There is no workaround.

- 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.

- CSCsm84257

  Symptoms: A Catalyst 6500 or a Cisco 7600 may reload unexpectedly. On the console or in the RP crashinfo file, the following message can be seen:

  ```
  %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Per-Second Jobs.
  ```

  Conditions: This has been seen on a Cisco 7600 running Cisco IOS Release 12.2(33)SRC and 12.2SXH. The bug can occur for 6500 and 7600.

  Workaround: Disable Netflow by using one of the following commands on every sub-interface for which Netflow is configured.

  no ip flow ingress

  no ip flow egress

no ip route-cache flow

- CSCsm84849

  Symptoms: The **priv** option is not under the **snmp- server group** *name* **v3** command.

  Conditions: In a Cisco 7200 crypto image, the **priv** option is not present when user tries to configure the **snmp-server group** *name* **v3** command.

  Workaround: There is no workaround.

- CSCsm86039

  Symptoms: After switchover, DHCP relay is unable to forward the DHCP REQUEST received from client during RENEW to the server.

  Conditions: Occurs when unnumbered DHCP relay with server address configured under class submode in relay pool config mode.

  Workaround: Configure the server address directly under relay pool mode (rather than class submode) or under the interface (helper address).

- CSCsm86236

  Symptoms: The standby RP reloads continuously.

  Conditions: This occurs on a router in the SSO mode when the **no address-family <name> command is followed rapidly by a address-family <name>** command in the "vrf definition" sub-mode.

  Workaround: Wait for a few seconds to reconfigure the address family after deconfiguring it.

- 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.

- CSCsm88496

  Symptoms: MPLS disposition traffic on ESM20 may get dropped.

  Conditions: Occurs with scaled EVC and VPLS/EOMPLS configuration after several line card online insertion and removal (OIR) events and then an SSO.

  Workaround: Toggle MPLS configuration on the interface that has the issue occur.

- 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.

- CSCsm90366

  Symptoms: IP Multicast cannot be L3 switched between two routed pseudowires.

  Conditions: Occurs when 7600-SIP-600 or 7600-ES-20 are used as the EoMPLS imposition card. IP multicast traffic will be dropped when the incoming and outgoing interface are both routed pseudowires. IP unicast traffic is not affected.

  Workaround: There is no workaround.

  Further Problem Description: VPLS/EoMPLS check for split-horizon forwarding does not work properly when the packet has been L3 Multicast switched. The split-horizon check is intended to be bypassed when the packet has been L3 switched as is the case for routed PW feature. However, that check does not work properly for L3 multicast switching.

  Cisco IOS Release 12.2(33)SRB3 is unaffected. The issue does, however, apply to Cisco IOS Release 12.2(33)SRC.

- CSCsm90525

  Symptoms: Under certain scenarios when deploying Multicast extranets, a change in the unicast routing information can cause the router to unexpectedly crash.

  Conditions: This issue is only seen when Multicast extranets are deployed.

  Workaround: There is no workaround.

- CSCsm91084

  Symptoms: Link flaps may be observed on a TenGigabitEthernet interface with XENPAK-10GB-LW under load.

  Conditions: This was observed under a high-traffic test scenario of over 9 Gb traffic rate.

  Workaround: Reduce traffic load. The XENPAK-10GB-LW will not support greater than 9 Gbps of traffic.

- CSCsm92365

  Symptoms: Cisco 7600 series router loses its VLAB database after configuring VTPv3.

  Conditions: This bug is observed on a Cisco 7600-RSP7203CXL router running IOS version Cisco IOS Release 12.2(33)SRC.

  Workaround: There is no workaround.

Further Problem Description: The customer is upgrading from 12.2(33)SRB2 to 12.2(33)SRC. Initially the router is running VTPv2 on 12.2(33)SRB2 and the router is reloaded with 12.2(33)SRC and the VTP version remains at V2. At this point the VTP config and VLANs are as they were on SRB2. Now the VTP version is changed from V2 to V3 and the router is reloaded. On reload with 12.2(33)SRC with VTP version 3, all the VLANs disappear.

- CSCsm92389

  Symptoms: With “switchport mode dot1q-tunnel” configured, if a user explicitly configures “spanning- tree bpdufilter disable”, on a interface flap or a interface shut/no shut, “spanning-tree bpdufilter disable” configuration will be replaced with “spanning-tree bpdufilter enable”.

  Conditions: This bug happens with dot1q-tunnels and on shut/no shut.

  Workaround: Reapply “spanning-tree bpdufilter disable”.

- CSCsm92916

  Symptoms: When the number of VCs configured for out-of-band clock master are not continuous, the SPA might not generate packets for some of the clock master VCs.

  Conditions: Occurs on the following hardware: * SPA-24CHT1-CE-ATM * SPA-1CHOC3-CE-ATM * SPA-2CHT3-CE-ATM

  Workaround: Configure out-of-band clock master so that the number of VCs are continuous.

- 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.

- CSCsm93088

  Symptoms: After a flap or disconnection/restoration of T1s, random Multilink bundles on Cisco 7606 running Cisco IOS Release 12.2(33)SRB2 are up, but traffic does not pass through it when working with a third-party device.

  Conditions: Problem of interoperatibility when working third-party device, the problem is present with the flap of T1 lines. When the T1s are restored, there is a problem with the synchronization on the sequence numbers.

  Workaround: Delete and reconfigure again the bundle or reset the line card.

- 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.

- CSCsm94366

  Symptoms: Device crashes after doing steps that are seen in conditions.

  Conditions: This issue would require many steps such as removing subinterfaces; reconfiguring the device; attaching a policy-map to ATM main interface two times; and then performing an OIR operation.

  Workaround: There is no workaround. Some of the steps and the whole sequence are not typical at customer environment.

- CSCsm94385

  Symptoms: Netflow entry left as part of residue in a diagnostic test.

  Conditions: This symptom is observed on a fully loaded chassis with ESM20G 2X10GE and 20X1 and is seen to leave a net flow entry as a residual of the test due to which traffic is getting disturbed.

  Workaround: A temporary fix is provided by skipping the test from the diagnostic suite.

- CSCsm94533

  Symptoms: Traffic might fail on dMLP bundles when SPA online insertion and removal (OIR) is done.

  Conditions: Occurs when a SPA is OIRed on a SIP-200 on a Cisco 7600 router having dMLP bundles with member links from a SPA.

  Workaround: Perform a OIR of the SIP-200 line card to bring the traffic up.

- 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.

- CSCsm95041

  Symptoms: Standby RP crashes when two users are logged into the router.

  Conditions: Occurs when two users are logged into the router at the same time. The first user is logged into the router via Telnet and issues the **show startup-config** command and the user does not exit the config. Meanwhile a second user Telnets into the box, makes some config changes and issues the write command. The second user's Telnet session hangs for approximately 5 minutes. After this period the standby RP crashes.

  Workaround: There is no workaround.

- CSCsm95145

  Symptoms: On a Cisco 7206VXR (NPE-G2) processor that is running Cisco IOS Release 12.2SRC, only one of the two prepaid services is downgraded on credit- exhaust event on both the prepaid services.

  Conditions: This issue is seen for a configuration where multiple prepaid services are being used, and separate actions are configured for credit- exhaust for those services. For example:

  ```
  policy-map type control RULEB
    class type control MATCH_PRE_1 event credit-exhausted
  ```

```
 1 service-policy type service name DOWN_DEF_TC1_V1
!
class type control MATCH_PRE_2 event credit-exhausted
 1 service-policy type service name DOWN_DEF_TC2_V1
!
```

Workaround: There is no workaround.

- CSCsm96762

  Symptoms: Memory fragmentation at l2tp_session_app_notify_incoming sessions fails. Memory leaks will appear in AAA_ACCT_DB, AAA_GENERAL_DB.

  Conditions: This symptom occurs only when the **vpdn session accounting network** default CLI is configured. The leak depends on the number of sessions.

  Workaround: There is no workaround.

- CSCsm97560

  Symptoms: MCL check failure is seen with **upgrade fpd auto** command.

  Conditions: The problem is seen when performing ISSU downgrade from an IOS release supporting the FPD feature to the one that does not support the FPD feature.

  Workaround: Add the **upgrade fpd auto** command to the MCL ignore list.

- CSCsm97911

  Symptoms: On a Cisco 7206VXR (NPE-G2) processor that is running Cisco IOS interim Release 12.2(33.0.6)SRC (c7200p- advipservicesk9_li-mz.122-33.0.6.SRC), ARP keepalive is not found to be supported.

  Conditions: This symptom is observed a a Cisco 7206VXR (NPE-G2).

  Workaround: There is no workaround.

- CSCsm98000

  Symptoms: ISSU upgrade procedure takes switch into RPR instead of SSO.

  Conditions: Occurs when trying to use ISSU to upgrade a Cisco 7609 from Cisco IOS Release 12.2(33)SRB2 to Cisco IOS Release 12.2(33)SRC on Sup720 configured for SSO. After executing the “issu runversion 6” which will reload the active, the switch goes into RPR redundancy with current active one having the new image SRC and the other one with the old SRB2 as the standby.

  “%PFREDUN-SP-4-INCOMPATIBLE_ISSU_MATRIX: Compatibility Matrix check failed. reason 3” is recorded in logs despite the execution of the command **no service image-version efsu** prior to the upgrade.

  Workaround: There is no workaround.

- CSCsm99651

  Symptoms: Link down notification is slow on ES-20.

  Conditions: Occurs on 10GE ports of ES-20 line card, when fiber is removed to simulate link failure, it might take up to 3 seconds for MPLS TE FRR to respond. Issue is intermittent.

  Workaround: Shutdown the port on the remote device.

- CSCsm99690

  Symptoms: Router crashing when it tries to export with Netflow Version 9 format.

Conditions: Router is configured with Netflow Version 9 on aggregation and netflow main cache. Problem is seen when aggregation caches are configured, and export is configured to one collector in the global table and one collector in a VPN.

Workaround: Do not use Netflow Version 9.

Further Problem Description: Netflow Version 9 configuration should be configured with destination. When Version 9 configuration and unconfiguration tried on aggregation and main cache many times may lead to crash due to reset of aggregation functionalities set to NULL.

- CSCsm99975

  Symptoms: Routers running Cisco IOS Release 12.2(33)SRC are experiencing module resets when another router is being reset. All modules on all routers running this image are reset, excluding the Supervisor Engine 720 module.

  Conditions: Occurs on Cisco 7606 and Cisco 7609 router with 67XX modules with DFC3BXL. IPv6 is configured on interfaces on those modules and crash decodes point to IPv6.

  Workaround: There is no workaround.

- CSCso02266

  Symptoms: Cisco 7600-SIP-600 may crash when carrying a EOMPLS or VPLS VC's over TE/FRR tunnels.

  Conditions: Crash may be observed when the primary TE path goes down.

  Workaround: Avoid TE/FRR configuration for EOMPLS/VPLS VC's on sip600.

- 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.

- CSCso06409

  Symptoms: A Cisco 7600 (RSP720-3C/CXL) may experience high CPU utilization from the moment (S,G) expires due to all outgoing interfaces are down.

  Conditions: This symptom occurs when indirect-connected multicast source traffic arrives at PIM-RP router without any receiver on that group, a (*,G) state with NULL RPF interface and NULL OIL is created and used to forward the traffic. Because of NULL RPF, this (*,G) state cannot be installed in Cisco 7600 hardware. The multicast data packet is punting to CPU and causes high CPU utilization.

  Workaround: Partial workaround is to apply RP rate-limiter with fib-miss option.

- CSCso07811

  Symptoms: Remote-id and circuit-id are no longer formatted as Type Length Value (TLV) in radius packets.

  CLI command to enable legacy behavior (formatting remote-id and circuit-id)

  1. config t
  2. subscriber policy format_option82_for_cats

  New behavior:

```
remote id 00046aacfc82
 circuit id 00000009
```

Radius see it as:

```
*Apr 16 05:33:30.695: RADIUS:  User-Name           [1]   16  "aabb.cc00.6500"
 *Apr 16 05:33:30.695: RADIUS:  User-Password       [2]   18  *
 *Apr 16 05:33:30.695: RADIUS:  Calling-Station-Id  [31]  14  "00046aacfc82"
 *Apr 16 05:33:30.695: RADIUS:  NAS-Port-Type       [61]  6
 Virtual                   [5]
 *Apr 16 05:33:30.695: RADIUS:  Vendor, Cisco       [26]  31
 *Apr 16 05:33:30.695: RADIUS:   Cisco AVpair       [1]   25  "circuit-id-
 tag=00000009"
 *Apr 16 05:33:30.695: RADIUS:  Vendor, Cisco       [26]  34
 *Apr 16 05:33:30.695: RADIUS:   Cisco AVpair       [1]   28  "remote-id-
 tag=00046aacfc82"
 *Apr 16 05:33:30.695: RADIUS:  NAS-Port            [5]   6
 0
```

Legacy behavior:

```
remote id 00046aacfc82
 circuit id 00000009
```

Radius see it as: (note the extra characters)

```
RADIUS:  Calling-Station-Id  [31]  15  "0|4|6aac.fc82"
RADIUS:  NAS-Port-Type       [61]  6
 Ethernet                  [15]
RADIUS:  Vendor, Cisco       [26]  32
RADIUS:   Cisco AVpair       [1]   26  "circuit-id-
 tag=0|0|9|2|6"
RADIUS:  Vendor, Cisco       [26]  35
RADIUS:   Cisco AVpair       [1]   29  "remote-id-
 tag=0|4|6aac.fc82"
RADIUS:  NAS-Port            [5]   6
 16777329
RADIUS:  NAS-Port-Id         [87]
 25  "0|4|6aac.fc82:0|0|9|2|6"
```

Workaround: There is no workaround.

- CSCso09237

  Symptoms: A Cisco 7200 router crashes due to memory corruption.

  Conditions: This symptom occurs when issuing “no ip routing” using a SSH session.

  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.

- CSCso09791

  Symptoms: When configuring an incorrect de-jitter buffer value on CEM interface, the CEM group will stay down and not recover until the SPA is reloaded.

  Conditions: This symptom only occurs if the de-jitter is out of range. Acceptable range is as follows:

# DS0s	max pay	max j(ms)	min j(ms)	min pay	max j(ms)	min j(ms)
1	40	320	10	32	256	8
2	80	320	10	32	128	4
3	120	320	10	33	128	4
4	160	320	10	32	64	2
5	200	320	10	40	64	2
6	240	320	10	48	64	2
7	280	320	10	56	64	2
8	320	320	10	64	64	2
9	360	320	10	72	64	2
10	400	320	10	80	64	2
11	440	320	10	88	64	2
12	480	320	10	96	64	2
13	520	320	10	104	64	2
14	560	320	10	112	64	2
15	600	320	10	120	64	2
16	640	320	10	128	64	2
17	680	320	10	136	64	2
18	720	320	10	144	64	2
19	760	320	10	152	64	2
20	800	320	10	160	64	2
21	840	320	10	168	64	2
22	880	320	10	176	64	2
23	920	320	10	184	64	2
24	960	320	10	192	64	2
25	1000	320	10	200	64	2
26	1040	320	10	208	64	2
27	1080	320	10	216	64	2
28	1120	320	10	224	64	2
29	1160	320	10	232	64	2
30	1200	320	10	240	64	2
31	1240	320	10	248	64	2

  Workaround: The CEM group will come up when:

  - De-jitter is reconfigured in acceptable range
  - CEoP SPA is reloaded.

- 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.

- CSCso10933

  Symptoms: CE to CE connectivity is broken when MPLS over TE is configured.

  Conditions: With this toploogy,CE1--PE1 -P-PE2-CE2, VRF VPN is configured between CE1-PE1, CE2-PE2. TE tunnels from PE1 to PE2 and PE2 to PE1. With this scenario, ping from CE1 to CE2 fails.

  Workaround: There is no workaround.

- CSCso11822

  Symptoms: Sometimes the “channel-group” configuration is lost from member ports of a primary aggregator on removal and reinsertion of a line card.

  Conditions: The LACP port-channel should have member ports belonging to a primary aggregator on the line card that is removed and reinserted. This problem happens intermittently only when primary and secondary aggregators are present.

  Workaround: There is no workaround.

- CSCso12748

  Symptoms: Tunnels between Cisco and non Cisco peers fail to come up since the Mandatory of Message Type AVP for SCCRQ that is sent by Cisco is FALSE.

  Conditions: This symptom occurs because the Mandatory of Message Type AVP for SCCRQ that is sent by Cisco is FALSE.

  Workaround: There is no workaround.

- CSCso13791

  Symptoms: OSPF neighbor adjacency is formed and lost over a QinQ subinterface every few minutes. This may keep happening indefinitely. Traffic forwarding on this subinterface is affected as OSPF adjacency flaps.

  Conditions: This problem is observed in a Cisco 7600 series with an RSP720 Supervisor Engine if OSPF has been configured on a QinQ subinterface on an ES20 or ES40 module. The problem is not seen if single tag encapsulation is used.

  Workaround: There is no workaround.

  Further Problem Description: On a subinterface that is configured with a QINQ encapsulation in a system with an RSP720 supervisor, protocol packets will be dropped, so this will affect other layer 3 protocols in addition to OSPF.

- CSCso14979

  Symptoms: Distributed CEF gets disabled for a line card.

  Conditions: This symptom can happen for a few reasons:

  1) Heavy IPC load leading to backplane congestion causing timers (started to monitor distribution) to time out.

  2) Breakdown of IPC communication between the RP and the line card.

3) Lack of memory to install FIB updates on the line card.

Workaround: The only way to restart distributed CEF for the disabled line card is by resetting or OIR the line card.

- 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.

- CSCso19075

  Symptoms: From SNMP, using MIB object cRFCfgAdminAction.0 to perform SSO does not work. The effect is no switchover is performed.

  Conditions: This symptom happens when user tries to use SNMP to initiate a switchover.

  Workaround: Use the **redundancy** command instead of the **snmp** command.

- CSCso20519

  Symptoms: There is some probability of Cisco IOS bootup failures on the Cisco 7600-SSC-400.

  Conditions: The failures are seen at cold temperature corners in testing. There are no failures reported from the field.

  Workaround: There is no workaround.

- CSCso21611

  Symptoms: Device crashes due to memory allocation issue.

  Conditions: Observed on Cisco 7200, but this is not a platform-specific bug.

  Workaround: There is no workaround.

- CSCso21888

  Symptoms: Router may spontaneously reload.

  Conditions: Occurs on routers configured with iSPF computation algorithm in OSPF.

  Workaround: Disable iSPF.

- CSCso22098

  Symptoms: OSPF neighborship goes down on RPR+ switchover on core router. The router does not send any hello packets to the connected routers.

  Conditions: Occurs when executing RPR or RPR+ switchover. No Problem seen with SSO switchover.

  Workaround: There is no workaround.

- CSCso22328

  Symptoms: If you have a ip-session l2-connected your interface config will show “ip subscriber l2-connected” and, you are redirecting a session upon session start event for a web-portal-log-on

  !

```
policy-map type control web-logon
 class type control always event session-start
  10 service-policy type service aaa list BH-125 name L4_SERVICE
```

```
  20 service-policy type service aaa list BH-125 name PBHK_SERVICE
 !
 class type control always event account-logon
  10 authenticate aaa list WEB_LOGON
  20 service-policy type service unapply name L4_SERVICE
```

Upon doing account-log-on form the portal, ISG does not include attribute 31 = mac-address in access-request sent to AAA.

Conditions: When doing web-log-on using CoA Account-log-on , access-request is missing attr-31, example:

```
Mar 14 12:35:07.462: RADIUS(00000273): Send Access-Request to 10.30.81.21:1812 id
1645/74, len
252
Mar 14 12:35:07.462: RADIUS:  authenticator 06 CA 9B E6 63 13 A9 DD - 6C BC C9 ED E5
74 19 49
Mar 14 12:35:07.462: RADIUS:  User-Name           [1]   10  "easy-vrf"
Mar 14 12:35:07.462: RADIUS:  User-Password       [2]   18  *
Mar 14 12:35:07.462: RADIUS:  Calling-Station-Id  [31]  16  "0002.1760.E1C3" << << <<<<
```

This may be a problem for some policy managers.

Workaround: There is no workaround.

- CSCso23419

  Symptoms: The CBTS master tunnel goes down on rare occasion when the path change occur on all the members. Even after a member tunnel comes up, the master tunnel does not report up for 10 seconds.

  The CBTS members are configured with the same sequence of explicit path-options. When the link down occur on head-end on the LSP path, the new LSP are setup as the next-path on all the members in this case.

  This only impacts the reporting of the master tunnel state.

  Conditions: Configure the same sequence of explicit path-options on all the members.

  Workaround: There is no workaround.

- 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.

- 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).

- CSCso25936

  Symptoms: HQoS policy-map does not take effect for 10 minutes after line card (ESM20) OIR.

  Conditions: This symptom occurs after line card OIR when the HQoS policy has been applied to an interface.

Workaround: There is no workaround.

- CSCso26664

  Symptoms: Single clock source would not recover when frequency was brought back in during wander test.

  Conditions: This symptom occurs when wander testing during compliance testing.

  Workaround: Delete clock source and reconfigure.

  Further Problem Description: This is not likely to happen in the field. If frequency drifts enough to fail the clock source, the interface or controller will likely fail. The controller or interface recovery would have triggered the DPLL to be configured in “normal” mode instead of staying in “holdover” mode.

- CSCso27913

  Symptoms: Router crashes doing write memory with color-aware policer configuration.

  Conditions: Removing a class-map which is referenced in a color-aware policer is the trigger. Related to **conform-color** command. The color-aware policer is left pointing to freed memory. A show running after this causes the crash.

  Workaround: Remove color-aware policer configuration before removing the class-maps to which it references.

- 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*.

- CSCso30946

  Symptoms: Line card does not come up first time with image download failure with the following error message:

  ```
  %ONLINE-SP-6-DNLDFAIL: Module <slot>, Proc. 0, Runtime image download failed because
  of scp send failure
  ```

  Conditions: This is mainly seen when multiple line cards removed and inserted at the same time.

  Workaround: There is no workaround.

- CSCso32982

  Symptoms: NSE-100 processor crashes while bringing up L2TPV3oATM-FR circuit.

  Conditions: It occurs consistently when we bring up L2TPV3oATM-FR.

  Workaround: There is no workaround.

- CSCso33003

  Symptoms: If a child policy is attached to a parent policy twice, the router will reload if child policy configuration is removed.

  Conditions: The parent policy needs to be attached to target interface.

  Workaround: Do not attach the same child policy twice in the same parent policy. Use different policy instead.

- 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.

- CSCso35876

  Symptoms: Supervisor or DFC line card crash in cmfi_qos_walk_apply_func.

  Conditions: This issue is seen very rarely.

  Workaround: There is no workaround.

  Further Problem Description: When this problem is observed collect the crashinfo from the Supervisor Processor (SP) or the DFC line card.

- 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.

- CSCso38907

  Symptoms: ATM VCs are inactive after a line card OIR followed by a PRE switchover before the line card finishes booting up.

  Conditions: This symptom is seen with ATM line cards.

  Workaround: A **shut** followed by a **no shut** cycle clears the problem.

- 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.

- CSCso40536

  Symptoms: POS interfaces keep flapping.

  Conditions: This symptom is observed while doing an upgrade to Cisco IOS Release 12.2(33)SB. After using the **issu runversion** command, POS interfaces keep flapping.

  Workaround: Using the **hw-module reset** command brings up the POS interface stable.

- CSCso44120

  Symptoms: Unable to perform SNMPwalk of clcFdbVlanInfoTable.

  Conditions: Occurs all the time.

  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.

- CSCso49598

  Symptoms: Standby reloads continuously when “MAXINT” is used with “int ran” to create logical interfaces using.

  Conditions: Occurs in SSO mode.

  Workaround: Avoid giving MAXINT as range.

  Further Problem Description: At a stretch, only 1000 logical interfaces could be created through interface range. Due to some wrap-around problem, it was not showing error when MAXINT was given as option and starts creating these many interfaces which are much beyond the MAXINTERFACES supported by any existing platform. It will lead to MEMORY getting exhausted and different after effects as standby reload.

- CSCso50383

  Symptoms: In a Cisco 7600 ring topology with TE-FRR configuration, traffic might get software switched if the packet comes in on a interface and goes out of the same interface.

  Conditions: This can happen in a toplogy like the following:

  R1 ---------- R2 ---------- R3 | | |---------- R4 ----------|

  Link between R3 - R4 is protected via R3 -> R2 -> R1 -> R4 (typical ring topology). R1 and R3 are the end points of a VC. Normally traffic will take the primary TE tunnel via R-> R4 -> R1. When R3 -> R4 link is shut, traffic will go on the back tunnel, R3 -> R2 -> R1 -> R4. In R4, traffic will be sent back on the incoming interface to R1, VC destination. Now in R4 traffic will get punted to RP and route cached.

  Workaround: There is no workaround.

  Further Problem Description: These drops also ignore QoS markings and affect all service classes.

- 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.

- CSCso50794

  Symptoms: The **show spanning-tree vlan** *vlan id* **interface port-channel** *int id* command shows only option as EFP, and all other alternate options are not available.

  Conditions: The Symptom shows up whenever there is either port-channel interface or GigaEthernet interface.

  Workaround: There is no workaround.

- CSCso53489

  Symptoms: If you remove a policer from parent class of a hierarchical policy which also has policers in child policy, the policers get removed from the child policy as well. If you then add back the parent policer and show running, the router crashes.

  Conditions: Occurs with hierarchical policer configuration.

  Workaround: Detach policy from all interfaces before removing policer from parent class.

- CSCso55047

  Symptoms: Router crashes while unconfiguring **debug condition all** on L2TP network server (LNS).

  Conditions: This symptom occurs when **no debug condition all** is configured to remove the condition that was initially set.

  Workaround: There is no workaround.

- CSCso55072

  Symptoms: System traceback occurs during TCL code execution which causes subsequent system reboot.

  Conditions: Occurs when ESM is still processing events in the background and another syslog message is being processed from the ESM logger queue.

  Workaround: Avoid ESM filters that executes background events like CLI commands for an extended period of time, such as in a loop with high loop count.

- 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.

- CSCso55190

  Symptoms: Cisco 7600-SIP-400 crashes when changing the QoS scheduler configuration.

  Conditions: The crash has been observed on a Cisco 7604/MSFC2A/SUP32 running Cisco IOS Release 12.2(33)SRC.

  Workaround: There is no workaround.

- CSCso56101

  Symptoms: Some CFM remote MEPs may not appear as up when connected by a SIP-400 line card.

  Conditions: When a large number of remote MEPs are connected via an interface on a SIP-400 line card, they may not all appear.

  Workaround: There is no workaround.

  Further Problem Description: The remote MEPs are seen as CFM errors with a status of “lifetime timer expired” under the “show ethernet cfm errors” command.

- CSCso56185

  Symptoms: L2TP Start-Control-Connection-Reply (SCCRQ) and Start-Control-Connection-Reply (SCCRP) messages have incorrect setting of mandatory-bit for the receive window Size attribute-value pair (AVP). This may cause L2TP/VPDN sessions to fail to connect.

  Conditions: Occurs in VPDN environments where the peer requires tight protocol adherence.

  Workaround: There is no workaround.

- CSCso57001

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

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

  Workaround: There is no workaround.

- CSCso57407

  Symptoms: The standby Router resets and goes to RPR mode due to this config-sync issue. On Cisco 7600 platform upgrading an image from Cisco IOS Release 12.2(33)SRB to Cisco IOS Release 12.2(33)SRC may fail and the redundant routers will operate in RPR mode if the following command is configured under an interface.

  ```
  interface TenGigabitEthernet2/0/0
     l2protocol-tunnel drop-threshold lldp 20.
  ```

  The problem can be verified by executing the following show command.

  ```
  show redundancy config-sync failures mcl
   Mismatched Command List
   ----------------------
   interface TenGigabitEthernet2/0/0
    !  "interface"
   - l2protocol-tunnel drop-threshold lldp 20
    !  "interface"
  ```

  Conditions: The Cisco 7600 routers running Cisco IOS Release 12.2(33)SRB or Cisco IOS Release 12.2(33)SRC will observe the problem only if the configuration command **l2protocol-tunnel drop-threshold lldp 20** is configured under the interface.

  Workaround: The problem can be worked around by entering **no l2protocol-tunnel drop-threshold lldp 20** under the interfaces.

- CSCso57695

  Symptoms: Router reloads or hangs during process input policing.

  Conditions: Occurs when there is a single-level output queuing policy configured and a two-level input policing policy, not necessarily on the same interface.

Trigger: Repeated add/removal of policy from interface.

Problem Impact: Unable to reliably configure a combination of single level output queuing, 2 level input policing, and routing protocols.

Workaround: There is no workaround.

- CSCso59642

  Symptoms: ISIS, EIGRP & OSPF protocols are do not work when using ipbase image.

  Conditions: Occurs on the Cisco 7200 router.

  Workaround: There is no workaround.

- CSCso59736

  Symptoms: IOMEM depletion is observed on the router due to CMFI EoMPLS ICC message.

  Conditions: None.

  Workaround: There is no workaround.

  Further Problem Description: Note, not all IOMEM depletions are due to this issue. A deep inspection of the leaked buffers is required to link this issue to the one observed on the router.

  The first thing to do is find out which buffer pool is getting depleted by checking the number of buffers in the free list. Use the **show buffer** command to check this.

  Once the buffer pool is determined, dump the packets in the buffer using the **show buffer pool EOBC0/0 dump** command.

  This information will be good to analyze the packets on which application is holding on to or not releasing the buffers.

  If the router crashed due to the IOMEM depletion, then the crashinfo and debug_info file is required to analyze the issue properly.

- CSCso62915

  Symptoms: When adding a queueing policy-map to a Virtual Template on a Cisco 10000 series router that is acting as a LAC, the policy is not fully rejected. The box may crash due to an attempt to accept an invalid policy-map configuration.

  Conditions: This symptom is observed after creating a queueing policy-map and adding it to the Virtual Template configuration.

  Workaround: There is no workaround.

- CSCso66668

  Symptoms: Flexwan line card crashes in Cisco 7600 chassis.

  Conditions: Occurs when bre-connect is configured on an ATM PVC.

  Workaround: There is no workaround.

- CSCso66862

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

  Conditions: The crash is seen under the following conditions.

  1. Bringing up nearly 3k PPPoE and PPPoEoA sessions.
  2. Configuring **no interface virtual-template <no>** under ATM interfaces.

  Repeating Step 2 continuously will cause a crash.

Workaround: There is no workaround.

- CSCso68007

  Symptoms: Ethernet Out of Band Channel (EOBC) can halt on standby or active.

  Conditions: Occurs during very rare periods of EOBC traffic-intensive functions such as syncs between active and standby.

  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.

- CSCso74127

  Symptoms: PXF DMA crashes with the following error message:

  ```
  "End of Descriptor Before Cmd Byte Length Exhausted"
  ```

  Conditions: This symptom occurs when L2TP LNS with multicast is enabled on the session. Multicast source has to be from one of the L2TP sessions.

  Workaround: Limit multicast sources from L2TP sessions.

  Further Problem Description: See Root-Cause-Analysis.

- CSCso74156

  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. IPCP renegotiation fails on Client Router.

  Workaround: Within Cisco IOS Release 12.2(31)SB images, the cloning Virtual- Template interface did not require the **ip unnumbered X** command when running Cisco IOS Release 12.2(33)SB. The cloning Virtual- Template interface requires the **ip unnumbered X** command statement similar to the notation below:

  ```
  interface Virtual-Template201 ip unnumbered loopback201
  ```

- CSCso74503

  Symptoms: Ingress QoS does not work on the port-channel EVC after line card OIR.

  Conditions: While doing the OIR, there are some race conditions possible. QoS does not get applied on EVCs.

  Workaround: Remove and apply policy back on each EVC.

- 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.

- 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.

- 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.

- CSCso77116

  Symptoms: End to end connectivity is broken when pseudowire is configured on a port-channel interface or sub-interface and the member links are on LAN ports

  Conditions: xconnect has to be configured on the port-channel interface or sub-interface.

  Workaround: There is no workaround.

- CSCso80159

  Symptoms: IP Subscriber session ingress traffic is routed into incorrect VRF.

  Conditions: Occurs when the first access interface is up on a non-default VRF.

  Workaround: There is no workaround.

- CSCso81322

  Symptoms: User is not assigned IP Pool address received from AAA Server.

  Conditions: This symptom is seen when a different IP Pool is defined under the Virtual Template Interface than what is received via AAA Per User settings.

  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.

- CSCso87348

  Symptoms: A Catalyst 6500 or a Cisco 7600 may reload unexpectedly.

  Conditions: Occurs when NetFlow is configured on one of the following:

  – Cisco 7600 running Cisco IOS Release 12.2(33)SRC.
  – Catalyst 6500 running Cisco IOS Release 12.2SXH.

  Workaround: Disable Netflow. This is done with the following commands:

  no ip flow ingress

  no ip flow engress

  no ip route-cache flow

  Enter the appropriate command for each sub-interface for which NetFlow is currently configured.

- CSCso89464

  Symptoms: Command is rejected with the following error message

  `" interface range invalid, max 1000 interfaces allowed - command rejected".`

  Conditions: Occurs during the following sequence:

```
Router (config)# interface range create vlan 100
interface range invalid, max 1000 interfaces allowed - command rejected
```

Workaround: There is no workaround.

- CSCso92930

  Symptoms: Available memory may decrease over time on a Cisco ASR1000 RP as subscribers connect and disconnect.

  Conditions: This symptom is observed when the Cisco ASR1000 functions as a LAC or LNS. AAA accounting is enabled for tunnel, session and PPP.

  Workaround: If the available memory decrease impacts system functions, disable AAA accounting as a temporary remedy.

- CSCso93065

  Symptoms: Standby RP crashes while receiving dynamic sync from active RP during DHCP relay binding creation.

  Conditions: Occurs when outer is configured as DHCP relay and running IOS images that include the fix for CSCsm86039.

  Workaround: There is no workaround.

- CSCso97439

  Symptoms: The router crashes when doing OIRs.

  Conditions: This symptom is happening with Cisco IOS Release 12.2(32.9.25)SBf through Cisco IOS Release 12.2(32.9.25)SBc. The symptom is not seen with Cisco IOS Release 12.2(32.9.25)SBb.

  Workaround: There is no workaround.

- CSCso98143

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

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

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

  Workaround: There is no workaround.

- CSCsq02916

  Symptoms: A Cisco PA-MC-8TE1+ port adapter is not recognized.

  Conditions: This symptom is observed when a Cisco PA-Mc-8TE1+ port adapter is inserted on a Cisco 7200 series router with NPE-G1/NPE-G2 processor and Cisco 7301 router that is running ipbase/ipbasek9/spservicesk9 images.

  Workaround: There is no workaround.

- CSCsq05567

  Symptoms: Flow based CEF load-balancing does not work properly when the incoming interface is a multilink interface. The packets for the same flow are sent on a different Egress interface (different route is selected).

  Conditions: The problem is seen on a Cisco 10000 series router that is running Cisco IOS Release 12.2(31)SB and Release 12.2(33)SB images. The incoming interface for that particular flow is a multilink interface.

  Workaround: There is no workaround.

- CSCsq07492

  Symptoms: PXF crashes are observed on the Layer 2 Tunnel Protocol (L2TP) Network Server (LNS) when subinterfaces are removed on the L2TP Access Concentrator (LAC).

  Conditions: This symptom occurs on a Cisco 10000 series PRE-4 with L2TP tunnels configured.

  Workaround: There is no workaround.

- CSCsq07541

  Symptoms: Split horizon is not getting populated on standby member of the port channel.

  Conditions: Occurs when bridge domain with split horizon is configured and there is a standby member interface of the port channel.

  Workaround: There is no workaround.

- CSCsq07719

  Symptoms: The **sh mem deb leak chunks** command will display memory leaks on the Cisco 10000 series Spumoni SPA OIR process and State Machine Instance.

  Conditions: This symptom is seen on the Spumoni line card (jacket card with 4 bays) with any SPA plugged on it.

  Workaround: There is no workaround.

- CSCsq13938

  Symptoms: In Cisco IOS software that is running the Border Gateway Protocol (BGP), the router may reload if BGP **show** commands are executed while the BGP configuration is being removed.

  Conditions: This problem may happen only if the BGP **show** command is started and suspended by auto-more before the 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.

- CSCsq14340

  Symptoms: While reloading a Cisco router with dual RP with default start-up configuration of active RP, there is a stale **snmp mib community-map ILMI engineid** command seen in standby running configuration which is not seen in active RP configuration.

  Conditions: This symptom is observed in latest nightly build for Cisco IOS Release 12.2(33)SB image.

  Workaround: There is no workaround.

- 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.

- CSCsq18938

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

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

  Workaround: Disable health monitoring tests on the WS-6708

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

  ```
  %PIM-5-NBRCHG: neighbor 10.252.3.130 DOWN on interface Port-channel10 non DR
  %CONST_DIAG-SP-6-HM_TEST_SP_INFO: TestFabricCh0Health[3]: last_busy_percent[8%],
  Tx_Rate[894], Rx_Rate[2454]
  %CONST_DIAG-SP-2-HM_MOD_RESET: Resetting Module 3 for software recovery, Reason:
  Failed TestFabricCh0Health
  %OIR-SP-3-PWRCYCLE: Card in module 3, is being power-cycled off (Diagnostic Failure)
  ```

- 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.

- 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.

- CSCsq31580

  Symptoms: WRED does not work on MLPoLNS bundle.

Conditions: This symptom occurs if a class configured with WRED is applied to a MLPoLNS bundle and if downstream traffic is sent on that class. All the packets go through the default profile.

Workaround: There is no workaround.

- CSCsq31923

  Symptoms: Crash may occur after polling MPLS-LSR-MIB mplsInterfaceConfTable.

  Conditions: MPLS-enabled tunnels exist in configuration and some are removed by doing **no int tunnel** *tunnelid*. If mibwalk of any object in mplsInterfaceConfTable is performed after that, this may result in crash.

  Workaround: Remove MPLS configuration on tunnel with the **no tunnel mode mpls traffic-eng** command before entering the **no int tunnel** command.

  Further Problem Description: It has been found this problem occurs when tunnel also contains the following config: **tunnel mpls traffic-eng path-option 1 dynamic**. Crash occurs only if image contains fix for CSCsm97259. Will see this message similar to the following before the crash:

  ```
  %TIB-3-GENERAL: MPLS MIB subblock ifIndex corrupted for ifIndex: 46 - was: 1198404176;
  corrected
  ```

- 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#
```

- CSCsq77638

  Symptoms: When the **mtu** command is issued in VC mode, before the ATM PVC state sync, the MTU CLI is getting executed in the secondary RP. The secondary RP is accessing invalid memory, which causes the RP to crash.

  Conditions: The **mtu** command is expected to be used in subinterface mode. When this command is issued in VC mode, the secondary RP crashes.

  Workaround: Do not execute **mtu** command in VC mode. Execute in subinterface only.

- 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 “no aaa new-model” 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.

- 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.

Open Caveats—Cisco IOS Release 12.2(33)SB

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(33)SB. All the caveats listed in this section are open in Cisco IOS Release 12.2(33)SB. This section describes only severity 1, severity 2, and select severity 3 caveats.

Miscellaneous

- CSCek77178

  Symptoms: If a **clear ip bgp** *neighbor address* **soft out** command is issued for each iBGP neighbor with a 5+ second delay between them, the route will be cleared on the first iBGP neighbor but remains stuck on the other peers. Subsequent clear commands do not clear the remaining routes.

  Conditions: The symptom is observed when a BGP route is advertised to iBGP neighbors residing under the same peer group. A filter list is then applied to deny the route from going out to the iBGP neighbors. A **clear ip bgp** *neighbor address* **soft out** command is issued to each of the iBGP neighbors with a 5+ second delay. The route gets cleared for the first iBGP neighbor but does not clear for the remaining peers.

  Workaround: The route does not get stuck if the delay between the clear commands is removed.

- CSCse39643

  Symptoms: Route is not installed correctly in the router database. When the neighboring router receives it through RIP, the route is advertised back to the originating router. It then shows up in the originating router tables as a RIP route with a hop count of 2.

  Conditions: This symptom occurs on a Cisco 7200 router that is running Cisco IOS Release 12.2(32)SB and using RIP as the PE-CE routing protocol in an MPLS VPN. This may also occur on a Cisco 10000 router.

  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.

- CSCsg81628

  Symptoms: 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"
  ```

  Conditions: The crash is seen on a Cisco 10000 platform that is running Cisco IOS Release 12.2(31)SB8. Previous Cisco IOS versions are potentially affected.

  Workaround: There is no workaround.

- CSCsh91015

  Symptoms: Tracebacks are seen on **shut/no shut** of ATM-Ethernet local-switched connection. Also traffic does not go through the connection after the **no shut**.

  Conditions: This symptom happens only after a **shut/no shut** on the connection.

  Workaround: Remove and reapply the connection with no connect/connect.

- CSCsi18449

  Symptoms: All L2TP Ethernet circuits will not come up when we scale above 3k L2TP-over Ethernet.

  Conditions: This symptom occurs when we scale above 3K L2TP-Ethernet circuits. It works fine around 2k circuits.

Workaround: There is no proper workaround. If we can scale down to 2k, it will work

- CSCsi30175

  Symptoms: A Cisco 7200 router may return “Success” for an LI intercept instead of “Error Code 404 (Invalid Request)” when an invalid intercept is placed.

  Conditions: The defect might be observed when the LI intercept-Identifier is greater than 8 octets and encryption is used on Cisco 7200 platform.

  Workaround: Do not use encryption.

  Further Problem Description: The problem is not seen on Cisco10000.

- CSCsi76729

  Symptoms: BGP neighbors are not coming up in a multicast RPF scenario with PXF.

  Conditions: This symptom is observed on a Cisco 7304 NSE 100 platform.

  Workaround: Disable PXF.

- CSCsi91794

  Symptoms: Multicast ping packets are dropped on far end PE router with PXF enabled.

  Conditions: This symptom only happens on Cisco 7300 NSE100.

  Workaround: There is no workaround.

- CSCsj21785

  Symptoms: TE (Traffic Engineering) Tunnel does not reoptimize to explicit path after MTU change.

  Conditions: 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 reoptimizes to a dynamic path-option as expected. Now the MTU is reverted back to previous value, and the OSPF adjacency comes up. The TE Tunnel does not reoptimize to explicit path. Manual reoptimization of the TE tunnel fails as well, and the TE tunnel sticks to the dynamic path.

  Workaround: Perform shutdown/no shutdown on the particular interface:

  Shutdown

  no Shutdown

- CSCsj25315

  Symptoms: When /128 IPv6 route is added and withdrawn, watchdog expire may occur on a Cisco 10000 router that is running Cisco IOS Release 12.2(33)SB.

  Conditions:

  1. There are a lot of prefix-length /128 routes.
  2. There are more than 2 summary routes covering above /128 routes.
  3. There is a routing flap with summary route which is longer prefix.

  Workaround:

  1. Reduce the number of /128 routes.
  2. Prevent summary route flap. For example, configure static summary route to Null interface.

- CSCsj51401

  Symptoms: PPPoX sessions with QoS may experience irregular session recovery when a LAC BRAS router undergoes conditions such as flapping interfaces or operator initiated flapping of sessions. When the LAC router encounters negative conditions (flapping interfaces or sessions, etc.), not all sessions with QoS will get re-established.

  Conditions: This symptom is observed in a LAC-LNS environment on Cisco 10000 series routers that have PRE-3(s) but may not be limited to this platform. Problem does not occur when QoS is not configured on the sessions or client facing interface.

  Workaround: There is no workaround.

- CSCsk04318

  Symptoms: A Cisco 7600 router that is acting as standby RP will reload due to "address-family ipv4 vrf vpn1" parser return error.

  Conditions: Problem occurs after doing a switchover on Cisco 7600 router, and toggle the **address-family ipv4 vrf vpn1** command.

  Workaround: There is no workaround.

- CSCsk05653

  Symptoms: The **aaa group server radius** subcommand **ip radius source-interface** will cause the standby to fail to sync.

```
c10k-6(config)#aaa group server radius RSIM
 c10k-6(config-sg-radius)#ip radius source-interface GigabitEthernet6/0/0

 c10k-6#hw-module standby-cpu reset
 c10k-6#
 Aug 13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_NOT_PRESENT)
 Aug 13 14:49:31.793 PDT: %C10K_ALARM-6-INFO: ASSERT MAJOR RP A Secondary
removed
 Aug 13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_DOWN)
 Aug 13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_REDUNDANCY_STATE_CHANGE)
 Aug 13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_NOT_PRESENT)
 Aug 13 14:49:31.793 PDT: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_DOWN)
 Aug 13 14:49:31.813 PDT: %REDUNDANCY-3-IPC: cannot open standby port no such
port
 Aug 13 14:49:32.117 PDT: %RED-5-REDCHANGE: PRE B now Non-participant(0x1C11 =>
0x1421)
 Aug 13 14:49:32.117 PDT: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a
standby insertion (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

 Aug 13 14:50:52.617 PDT: %RED-5-REDCHANGE: PRE B now Standby(0x1421 => 0x1411)
 Aug 13 14:50:54.113 PDT: %C10K_ALARM-6-INFO: CLEAR MAJOR RP A Secondary
removed
```

```
 Aug 13 14:51:33.822 PDT: -Traceback= 415C75D8 4019FB1C 40694770 4069475C
 Aug 13 14:51:33.822 PDT: CONFIG SYNC: Images are same and incompatible

 Aug 13 14:51:33.822 PDT: %ISSU-3-INCOMPATIBLE_PEER_UID: Image running on peer
uid (2) is the same
 -Traceback= 415CCC2C 415C75FC 4019FB1C 40694770 4069475C
 Aug 13 14:51:33.822 PDT: Config Sync: Bulk-sync failure due to Servicing
Incompatibility. Please check full list of mismatched commands via:
   show issu config-sync failures mcl

 Aug 13 14:51:33.822 PDT: Config Sync: Starting lines from MCL file:
 aaa group server radius RSIM
  ! <submode> "sg-radius"
 - ip radius source-interface GigabitEthernet6/0/0
```

Conditions: This symptom is observed if the **aaa group server radius** subcommand **ip radius source-interface** CLI is configured on a box with dual PREs.

Workaround: If the customer does not use the **aaa group server radius** subcommand **ip radius source-interface** *interface*, this will not be a problem.

If they use the **aaa group server radius** subcommand **ip radius source-interface** *interface* on a Cisco 10000 router in simplex mode (a single PRE), this will not be a problem.

If they run with dual PREs, then they will need to remove the **aaa group server radius** subcommand **ip radius source- interface** *interface* from the configuration as a workaround.

Removing the **aaa group server radius** subcommand **ip radius source-interface** *interface* from the configuration could cause problems for the customer. The radius server may be expecting the request to come from a specific source address. The router will now use the address of the interface the packet egresses the router from, which may change over time as routes fluctuate.

- CSCsk40506

  Symptoms: NSE-100 crashes when we add/remove 500 mVPN config for multiple time while traffic is on.

  Conditions: This defect occurs when we add/remove multiple time through two telnet console, one is for adding mVPN and another for removing while the end to end traffic is on.

  Workaround: There is no proper workaround for this defect. If we avoid remove/add mVPN multiple time, it may not occur.

- CSCsk48412

  Symptoms: When a session profile provided via RADIUS contains instructions which cannot be implemented in the current Cisco IOS configuration, the client session may come up without the errant feature, or the entire session may fail to come up. The behavior varies among different Cisco IOS versions.

  There are no syslog, RADIUS accounting, or console logging to assist in locating the errors causing session failure or misconfiguration.

  Conditions: The failure of client sessions to be configured is due to the mismatch of what is configured in Cisco IOS and what is configured in the RADIUS database.

  Workaround: Verify the spelling of service policy-map names in RADIUS databases, comparing these with the service policy-map names in Cisco IOS configurations.

- CSCsk94713

  Symptoms: With Traffic Engineering tunnels configured on a NSE100 router with PXF enabled, the traffic status is not reflected in “sh int tunnel accounting” and the core interface of the LSP accounts the packets as IP packets instead of MPLS packets.

  Conditions: This symptom occurs with traffic engineering tunnel source being an NSE100.

  Workaround: There is no workaround.

- CSCsl61164

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

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

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

- 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.

- CSCsl93767

  Symptoms: Dynamically updating a hierarchical queuing policy on a session results in wrong traffic distribution to the classes.

  Conditions: The issue is seen on a PPPoEoVLAN session using integrated hierarchical queueing (shaping policy on the VLAN, HQoS policy on the session). Parent policy on the session has “bandwidth remaining ratio” configured.

  Workaround: There is no workaround.

- CSCsm36630

  Symptoms: Router crashes.

  Conditions: This symptom occurs when clearing PPPoE sessions while sessions are coming up with pushing policy maps via radius. A crash on a Cisco 10000 router is the result.

  Workaround: There is no workaround.

- CSCsm52088

  Symptoms: TFTP config takes 4 hours and finally times out.

  Conditions: This symptom happens on loading 30K IPoQinQ sessions via TFTP (15K sessions per port).

  Workaround: There is no workaround.

- CSCsm56140

  Symptoms: In an MR-APS environment, sometimes “working” channel CHOC12 card may get stuck in Signal Degrade state, forcing it to become a low priority link.

  Conditions: This symptom may been seen after long periods of traffic combined with several hw-module slot resets on a Cisco 10000 router that is running Cisco IOS Release 12.2(33)SB. It may also be seen when cable has been pulled and re-inserted into the active/working CHOC12 card.

Workaround: Working controller can be returned to a healthy state by doing one (or more) of the following:

- power-cycling router
- pulling/reinserting CHOC12 card
- pulling/reinserting cable at the ONS end

- CSCsm59217

  Symptoms: The Cisco 10000 box has APS configuration but reloads without redundant cards in the slots. The traffic fails to flow when the redundant cards are reinserted.

  Conditions: This symptom occurs when SR-APS is configured using 4XOC3atm cards in two back-to-back connected Cisco 10000 routers.

  Workaround: There is no workaround.

- CSCsm77227

  Symptoms: CPUHOG is seen on a Cisco 10000 router.

  Conditions: This symptom can occur during aggressive call setup with ISG PPPoX sessions, upon bootup, after power outage, or line card OIR.

  Workaround: There is no workaround.

- CSCsm95040

  Symptoms: On 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 occurs when modifying dsx3mode from PLCP to ADM or vice versa.

  Workaround: Remove all PVCs and re-define them or reload the line card.

- CSCso06402

  Symptoms: Unconfiguring the router may force the router crash where route-map is configured with DF bit set/unset.

  Conditions: A router may crash while unconfiguring, which has route-map configured with DF bit set/unset.

  Workaround: There is no workaround.

- CSCso09458

  Symptoms: SPAs in a MSC-100 go missing

  Conditions: Do **hw-module stop** then do a switchover and then **hw-module start** in new active.

  Workaround: Do a **hw-module subslot reload**.

- CSCso09680

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

  Conditions: This symptom occurs if the GRE tunnel has an output policy with set configured then CEF switching does not work.

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

- 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 condition occurs when PPP renegotiates an existing PPP connection on a Virtual-Access interface.

Workaround: Use Radius accounting for gathering statistics or billing where possible

- CSCso12748

  Symptoms: Tunnels between Cisco and non Cisco Peers fail to come up since the mandatory message Type AVP for SCCRQ sent by Cisco is FALSE.

  Workaround: There is no workaround.

- CSCso17319

  Symptoms: A 100% duplicate response may occur while multicast ping from CE-CE through GRE tunnel in MVPN scenario.

  Conditions: This symptom is observed on a Cisco 7304 NSE-100 platform.

  Workaround: Disable PXF.

- CSCso25148

  Symptoms: MLP bundle with greater than 8 member links does not dequeue on all members when traffic exceeds 80% of line rate with packet size less than 100 bytes.

  Conditions: This symptom is observed on a Cisco 10000 series with PRE3 when all of the following conditions are true:

  - Bundle with member links is greater than 8.
  - Traffic should be greater than 80% of bundle bandwidth.
  - Packet size of traffic is less than 100 bytes.

  This does not impact PRE2 as it uses VTMS. This does not impact PRE4 because of scheduler related changes for supporting 10G.

  Workaround: There is no workaround.

- CSCso25666

  Symptoms: On the CHOC12 and CHOC3 line cards, when issuing a controller **no path** command while T1s are configured under the T3, the line card might reload.

  Workaround: Delete all the T1s under the T3s before deleting the **path** command.

- CSCso26664

  Symptoms: Single clock source would not recover when frequency was brought back in during wander test.

  Conditions: This symptom occurs during Wander test during compliance testing.

  Workaround: Delete clock source and reconfigure.

  Further Problem Description: This is not likely to happen in the field. If frequency drifts enough to fail the clock source, the interface or controller will likely fail. The controller or interface recovery would have triggered the DPLL to be configured in “normal” mode instead of staying in “holdover” mode.

- 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 + Tos classification may work, but other classes in an ingress policy may not.

Conditions: This symptom is seen in Cisco 7300 or Cisco 10000 router that is running Cisco IOS Release 12.2(33)SB IOS code. It is not seen in Cisco 7200 router.

Workaround: Need to detach and reattach the policy-map to the interface.

- CSCso33454

  Symptoms:

  1. In a PE CE setup when 500 BGP VRF sessions are configured on a Cisco 10000, the PE PRE goes out of memory.
  2. In a PE CE setup when 600 BGP VRF sessions are configured on a Cisco 10000, the PE PRE goes out of memory and crashes.

  Conditions:

  1. The number of routes is 500*500 /31 routes and 500*220 /24 routes.
  2. The number of routes is 600*600 /31 routes.

  Workaround: There is no workaround.

- CSCso38907

  Symptoms: ATM VCs is inactive after a line card OIR followed by a PRE switchover before line card finishes booting up.

  Conditions: This problem applies to ATM line cards.

  Workaround: A **shut/no shut** cycle clears the problem.

- CSCso44328

  Symptoms: HDLC/PPP Layer2 VPN local switching circuits do not function.

  Conditions: This symptom can be seen on Cisco 7304 routers upon configuration of local switching.

  Workaround: There is no workaround.

- CSCso47448

  Symptoms: Connectivity between CE routers may break if PE router has configured with route-map that has match ACL and packet length.

  Conditions: This symptom is observed on a Cisco 7304 NSE-100 platform.

  Workaround: Disable PXF.

- CSCso50553

  Symptoms: After DS3ATM line card reloads, the ATM local switching circuit comes UP but no traffic is passing.

  Conditions: This symptom occurs when DS3ATM line card reloads on Cisco10000 router.

  Workaround: There is no workaround.

- CSCso62915

  Symptoms: When adding a queuing policy-map to a Virtual-Template on a Cisco 10000 router acting as a LAC, the policy is not fully rejected, and the box may crash due to an attempt to accept an invalid policy-map configuration.

  Conditions: This symptom is seen when creating a queuing policy-map. Add it to the Virtual-Template config.

Workaround: There is no workaround.

- CSCso67850

  Symptoms: When pasting (as in cut-and-paste) a set of IPv6 configuration CLI for a router network interface to the router console, the router may crash.

  Conditions: Unknown. The issue may occur during router configuration.

  Workaround: There is no workaround.

- CSCso74156

  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. IPCP renegotiation fails on Client Router.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SB

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(33)SB. This section describes only severity 1, severity 2, and select severity 3 caveats.

Miscellaneous

- CSCeb69473

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

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

```
router>connect 192.168.0.1 login /terminal-type aaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Trying 192.168.0.1...Open
login:

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

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

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

  Configuring Authorization
  http://www.cisco.com/en/US/docs/ios/12_4/secure/configuration/guide/schathor.html

  ACS 4.1 Command Authorization Sets
  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/ user/SPC.html#wpxref9538

ACS 4.1 Configuring a Shell Command Authorization Set for a User Group
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/ user/GrpMgt.html#wp480029

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

Role-Based CLI Access
http://www.cisco.com/en/US/netsol/ns696/networking_solutions_white_paper09186a00801ee18d.shtml

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_0900aecd804ac831.pdf

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

- 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.

- 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.

- 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.

- CSCek59453

  Symptoms: The spurious memory access may be generated on router.

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

  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.

- 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.

- CSCsd61498

  Symptoms: BGP bulk-syncs even in RPR+ mode. When the standby is reset, the BGP bulk-sync process continues to bulk-sync.

  Conditions: This symptom occurs during standby reset.

  Trigger: BGP bulk-sync process ignores notification.

  Impact: Traceback is observed when NSR neighbors are reset.

  Workaround: There is no workaround.

- CSCsd95616

  Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

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

- 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.

- CSCsg21394

  Symptoms: Router reloads unexpectedly by malformed DNS response packets.

  Conditions: This symptom occurs when configuring name-server and domain lookup.

  Workaround: Configure “no ip domain lookup” to stop the router using DNS to resolve host names.

- CSCsg78010

  Symptoms: The **show sss session detailed** command shows traffic for default TC as “Unmatched Packets (dropped)” irrespective of the configuration, e.g. whether default Traffic Class is set to forward or drop the traffic.

  Workaround: There is no workaround.

- CSCsi32646

  Symptoms: The following message may appear on the console after a line card reset or OIR:

  ```
  %UTIL-3-IDTREE_TRACE: PW freelist DB:Duplicate ID free ...
  ```

  Conditions: This symptom is observed when xconnects are configured on the line card interfaces and multiple RP switchovers have been performed.

  Workaround: There is no workaround.

- CSCsi70787

  Symptoms: A router may reset and generate a crashinfo file when memory that was allocated by a dead process is freed by another process.

  Conditions: This symptom is observed on an RPM-XF-512 that runs Cisco IOS Release 12.4T but is not platform-specific.

  Workaround: There is no workaround.

- CSCsj85065

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

  Cisco has released free software updates that address this vulnerability.

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

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

- CSCsj93012

  Symptoms: A Cisco 7500 router may crash when QoS is enabled.

  Conditions: This symptom occurs when ATM and serial interfaces have QoS configurations as output/input policy and when peer is reloaded.

  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.

- CSCsk26165

  Symptoms: A router may crash due to bus error.

  Conditions: The router must be configured for L2TP.

  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.

- CSCsk33724

  Symptoms: Starting with Cisco IOS Release 12.2(33)SXH, DOM feature will not be supported on some transceiver types. The list of supported transceiver types can be obtained from a running switch using the command **show interface transceiver supported-list**. This change has been made to handle cases where the DOM thresholds or operating values are inaccurate thereby resulting in bogus SNMP trap notifications.

  Conditions: This issue is seen only with the following conditions:

  1. Cisco IOS Release 12.2(33)SXH software and later only.
  2. Transceivers listed as “unsupported” in output of **show interface transceiver supported-list** command.

  Workaround: There is no workaround.

- CSCsk61686

  Symptoms: For an iEdge Traffic Class, defined by an ACL with greater than 1000 ACEs, the CPU will remain high for a few hours, and sessions do not come up.

  Conditions: This symptom can happen, for example, with a configuration of “L4R on TC” scenario with TC being based on an ACL with 5000 ACEs.

  Workaround: There is no workaround.

- CSCsk64223

  Symptoms: When “no router bgp xx” is configured, the following error message may be seen and the router may crash:

```
%IPRT-3-BAD_PDB_HANDLE: Pdb handle error 1040000, 0000, 0, 00000000, 76E60000, 00
-Process= "IP RIB
Update", ipl= 0, pid= 248
-Traceback= 4062C0A0 40CB7E08 40CD10D8 40CD1924
```

Conditions: This symptom occurs when BGP is enabled on a large number of VRFs and has a significant number of routes in each VRF.

Workaround: There is no workaround.

- CSCsk66339

  Symptoms: A Cisco 7600 router that is running Cisco IOS Release 12.2(18)SFX6 may encounter a condition such that when ISIS and Traffic Engineering are configured, ISIS should remove the native path from its local RIB and call RIB code to remove the path from global RIB but fails by either not passing the “delete” msg to RIB properly or RIB does not react when it received the “delete” call.

  Conditions: Show mpls traffic-engineering tunnel output may indicate “Removal Trigger: setup timed out” status.

  Workaround: **Shut/no shut** the interface or changing the metric temporarily to force an update:

  “tunnel mpls traffic-eng autoroute metric 1”

- CSCsk68846

  Symptoms: Router crashes when removing grandchild policy.

  Conditions: This symptom is seen in Cisco 7304 router.

  Workaround: There is no workaround.

- CSCsk71117

  Symptoms: The topo_name on the upgraded version remains null causing XDR to disable. All features that use XDR as their distribution mechanism will not work.

  Conditions: Software upgrade (ISSU) from SB9 to SR, i.e, from Pre-MTR release to Post-MTR release.

  Workaround: There is no workaround.

- CSCsk85987

  Symptoms: The line protocol state of SVI interfaces is incorrectly marked “down” after an SSO switchover.

  Conditions: This is sometimes seen on the second and subsequent SSO switchovers.

  Workaround: Reload the line card that has the affected interface.

- CSCsk86381

  Symptoms: Memory leak is seen in “Crypto IKMP” and “IPSEC key engine”.

  Conditions: This is observed in WS-C6509-E that is running engineering image s72033-advipservicesk9_wan-mz.NAT-D-5.

  Workaround: There is no workaround.

  Further Problem Description: This memory leak shows up in IPSEC process, but the fix is in IKE.

- CSCsk87523

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

  Conditions: This symptom occurs when configuring the following CLI on NAS:

  ```
  "radius-server host <ip add> auth-port 2295 acct-port 2296 test username sdanda
  idle-time 1 key cisco"
  ```

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

Impact: Display issue.

Workaround: There is no workaround.

- 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.

- CSCsl02927

  Symptoms: With no traffic on a PA-A6-OC3SMi card, the max ICMP pings times are seen at 352 ms 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 Cisco 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
```

- CSCsl04764

  Symptoms: Crash occurs when bringing up more than 2k DHCP class aware sessions.

  Conditions: This happens only when DHCP class aware is configured. Memory corruption might occur when multiple DHCP sessions are being brought up. The corrupting pattern is the DHCP classname.

  Further Problem Description: The memory corruption occurs when the configured DHCP class name is offered after the DHCP workspace for the particular DHCP discover message has been cleared.

- CSCsl04835

  Symptoms: A conditionally injected route is not removed from peers upon withdrawal.

  Consider this topology: RTR_A----------RTR_B----------RTR_C

  RTR_A advertises a prefix and RTR_B injects a more specific prefix of it.

  The problem is seen in two ways:

  1. If RTR_A withdraws the advertised prefix, the more specific prefix is removed on RTR_B, but this withdrawal is not sent to RTR_A and RTR_C.

2. If the conditional route injection configuration is removed on RTR_B, the more specific prefix is removed on RTR_B, but this withdrawal is not sent to RTR_A and RTR_C.

Workaround: There is no workaround.

- CSCsl05874

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

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

  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.

- CSCsl06336

  Symptoms: When the **maximum-paths** *n* **import** command is unconfigured, for example, a **no maximum-paths** *n* **import** *m* command is issued for a VPN/VRF on a router, sometimes the routes in that VPN may have duplicate path entries.

  For example:

```
diezmil#sh ip bgp vpnv4 v v1001 10.0.20.0
BGP routing table entry for 100:1001:10.0.20.0/24, version 1342275
Paths: (2 available, best #1, table v1001)
Flag: 0x420
  Not advertised to any peer
  65164, imported path from 100:1:10.0.20.0/24
    192.168.1.7 (metric 4) from 192.168.1.254 (192.168.1.254)
      Origin IGP, metric 1552, localpref 80833, valid, internal, best
      Extended Community: RT:100:1001
      Originator: 192.168.1.7, Cluster list: 192.168.2.7
      mpls labels in/out nolabel/291
  65164, imported path from 100:1:10.0.20.0/24
    192.168.1.7 (metric 4) from 192.168.1.253 (192.168.1.253)
      Origin IGP, metric 1552, localpref 80833, valid, internal
      Extended Community: RT:100:1001
      Originator: 192.168.1.7, Cluster list: 192.168.2.7
      mpls labels in/out nolabel/291
```

  Workaround: The least resource-intensive workaround is to configure and unconfigure a dummy import map under that VPN/VRF. Clearing the affected BGP sessions on PEs also resolves the issue.

- CSCsl11743

  Symptoms: Multilinks are down after a switchover.

  Conditions: This symptom is observed when dMLP and RPR+ are configured on a Cisco 7500 router, and a switchover occurs.

  Workaround: Micro-reload the Cisco 7500 router.

- CSCsl12315

  Symptoms: Router crashes.

  Conditions: Crash may occur after replacing OC12ATM card with a 6OC3POS card. Then doing “no card 6/0”. Replacing the 6OC3POS card with the OC12ATM card. Then doing “no card 6/0”. Then copying the original atm cfg to run via “copy startup-config running-config”.

  Workaround: There is no workaround.

- CSCsl17798

  Symptoms: EtherChannel membership on standby supervisor inconsistent with the state on active supervisor. Reported in ESM-20G line card.

  Conditions: This defect may be seen with EtherChannel mode is “on” and on a standby reload. This was reported in Cisco 7600 series router. Could impact other platforms.

  Trigger: EtherChannel configuration and performing SSO.

  Impact: This may impact traffic forwarding. EtherChannel state is inconsistent between active and standby.

  Frequency: Every time when line card reloads.

  Workaround: Once standby supervisor has reached hot, remove EtherChannel configuration and reapply.

- CSCsl20044

  Symptoms: PVC stays INAC.

  Conditions: The primary card of the APS pair should be shut and then released after SSO switchover on the new Active-PRE then PVCs stay DOWN.

  Workaround: There is no workaround.

- CSCsl27077

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

  Conditions: During the start of a PPPoA session with ISG configuration, Cisco IOS may experience a bus error and 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: There is no workaround.

- CSCsl27926

  Symptoms: For GRE tunnel inside VRF feature with source address in a different VRF, some times traffic will not flow through after an SSO switchover or DFC OIR for DFC having the ingress interface.

  Conditions: This symptom occurs when “tunnel vrf <vrf>” is configured on GRE tunnel and SSO switchover or DFC OIR is done.

  Workaround: There is no workaround. Reload router.

- CSCsl28246

  Symptoms: Not able to bring up more than 32768 TC Sessions and Out of IDs AAA trace back message is displayed.

  Conditions: This symptom occurs under TC sessions.

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

Trigger: While running ISG sessions with PPPoL2TP LAC/LNS on Cisco 10000, unable to bring up more than 32768 TC sessions because of the following Out of IDs AAA trace back 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 = 32768 IDs. Not able to bring up any more sessions because of accounting flow id allocation failure.

Workaround: Increase the number to number of sessions/flows required on the platform.

- CSCsl33632

  Symptoms: Router crashes when VRF is unconfigured.

  Conditions: Crash is observed on Cisco 7200 router while VRF is unconfigured.

  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.

- CSCsl38029

  Symptoms: After several thousand virtual private dial-up network (VPDN) sessions are created and torn down successfully, the router cannot create any new sessions. Either the L2TP Access Concentrator (LAC) or the L2TP Network Server (LNS) may fail with error message "VPDN Failed to obtain session handle." This error message will be seen only when you enable the **debug l2tp error** command.

  Conditions: The maximum number of successful sessions before failure varies by platform.

  Workaround: Reload the router.

- CSCsl40705

  Symptoms: Sometimes under stress situations the following tracebacks happen in VPDN.

  ```
  *Nov 20 06:19:57.771 IST: %IDMGR-3-INVALID_ID: bad id in id_to_ptr (bad id) (id:
  0x63249A94)
  -Traceback= 604721D4 60472718 6048C7B8 616C8CEC 616C9BA8 61AB48C4 61AB79A8 61AB8C48
  61AB8CAC 616C51DC


  Decodes:
  =======
  Enter hex value: 604721D4 60472718 6048C7B8 616C8CEC 616C9BA8 61AB48C4 61AB79A8
  61AB8C48 61AB8CAC
  616C51DC
  0x604721D4:verrmsg(0x604720b4)+0x120
  0x60472718:errmsg(0x604726c8)+0x50
  0x6048C7B8:id_to_ptr(0x6048c774)+0x44
  0x616C8CEC:l2tun_socket_db_get(0x616c8ccc)+0x20
  0x616C9BA8:l2tun_socket_session_get_client_context(0x616c9b94)+0x14
  0x61AB48C4:vpdn_get_session_from_socket_handle(0x61ab48ac)+0x18
  0x61AB79A8:vpdn_recv_CDN(0x61ab7980)+0x28
  ```

```
0x61AB8C48:vpdn_rcv_l2tun_socket_msg(0x61ab8bb0)+0x98
0x61AB8CAC:vpdn_process_msg(0x61ab8c8c)+0x20
0x616C51DC:l2tun_app_mgr_process(0x616c4f94)+0x248
Enter hex value:
```

Conditions: This symptom happens under stress situations when a CDN is received immediately after a connect request.

Workaround: There is no workaround

Further Problem Description: This a harmless traceback.

- CSCsl43546

  Symptoms: On the Cisco 7600 platform a reset of a line card may cause all MPLS over GRE adjacencies on the interfaces using that line card to be lost. Traffic will no longer be forwarded.

  Conditions: This problem can be caused on a Cisco 7600 by issuing the **hw-module** *module-number* **reset** command.

  Workaround: Reconfigure the interface to be admin down and then up. int <interface name> shutdown no shutdown.

- 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.

- CSCsl44497

  Symptoms: Class parameters cannot be configured under policy-map.

  Conditions: After attaching service policy to any interface, try changing the class parameters. It will not enter into class config mode.

  Trigger: Very basic functionality was broken.

  Workaround: Detach the service-policy from interface and modify class parameters and attach it back to the interface.

  Impact: Configuration issue.

- CSCsl45783

  Symptoms: See the CPUHOGs for 16k PPPoEQinQ sessions while passing the traffic.

  Conditions: There is no such specific command. However, there should be 16k sessions over 16k PPPoEQinQ subinterfaces. And those sessions should have L4R configured over them.

  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.

- CSCsl46959

  Symptoms: The router may hang and not be recoverable when reloaded with a specific config.

Conditions: The sequence that causes this condition requires that “ipv6 unicast-routing” be enabled before “ipv6 enable”. This can only happen during boot up when the MLD process has not started.

Workaround: There is no workaround.

- CSCsl47953

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

  Conditions: The issue appears to be restricted to the output of this particular show command. The output may be getting 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.

- CSCsl49124

  Symptoms: TCAM debug messages are observed while booting the router.

  Conditions: This symptom is seen on booting the router.

  Workaround: There is no workaround.

- CSCsl49167

  Symptoms: Continuous %IPC-5-WATERMARK: 884 messages pending in xmt for the port slot on 7600 SIP400. It affects any type of 7600 chassis and is not Specific to any Sup. The message are warnings that the buffer is being used up.

  Conditions: The problem occurs under high traffic conditions between RP and LC. The underlying EOBC transport encounters lots of collisions, which results in the WATERMARK message.

  Workaround: There is no workaround.

  Further Problem Description: The way it was reproduced was by pumping heavy traffic into IPC, and simulating congestion at the driver layer.

- CSCsl49628

  Symptoms: When a VRF is deleted through the CLI, the VRF deletion never completes on the standby RP and the VRF cannot be re-configured at a later time.

  Conditions: This symptom is observed when BGP is enabled on the router.

  Workaround: There is no workaround.

- CSCsl49705

  Symptoms: ISSU between SRB-2 & SRB-3 done, with tunnels configured on active, causes “IDBINDEX_SYNC-4-RESERVE” messages on standby (SRB-2) and a delay (wait) of around 3 sec per tunnel, which causes a standby reset in case there is a large number of tunnels configured.

  Conditions: This symptom occurs when tunnels are configured.

  Workaround: Remove tunnels configs before doing ISSU.

- CSCsl50471

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

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

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

- CSCsl50774

  Symptoms: Line card crashes repeatedly during boot after an unsuccessful FPD upgrade.

  Conditions: This symptom affects SRB and will prevent the line card from booting.

  Workaround: Once the line card is in the problem state, it cannot be recovered without this bug fix.

  Further Problem Description: The problem is that the recovery mechanism that is in place to correct for a mis programmed link FPGA needs an update.

- CSCsl51765

  Symptoms: The router crashes on doing a “no t1 channel-group”.

  Conditions: This symptom occurs when the “no channel-group” is issued on a CT3 SPA on a SIP400.

  Workaround: There is no workaround.

- CSCsl51945

  Symptoms: The HSRP IPv6 config on the standby RP may loose its address, such that the config on the standby RP appears as:

  standby 1 ipv6 ::

  The standby resets as well.

  Conditions: This will occur if group is in init state while doing the configuration or changes its state to init after applying the configuration. If you re-apply the command on the active RP without first removing it then a config sync error will occur and the standby RP will reload.

  Trigger: Standby RP on switchover stuck in standby-cold state.

  Impact: Secondary RP resets, configuration sync failure.

  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.

- CSCsl54616

  Symptoms: On-demand ATM VC of Cisco 10000 system is UP always on APS setup.

  Conditions: ATM VC shows UP all time with or without an associated PPP session. The ATM has APS.

  Workaround: Remove APS setup for the ATM interface.

- CSCsl54875

  Symptoms: The “test platform firmware get asic ....” command that is issued for a module may reset that module.

  ```
  Messages:
    00:27:15: %PM_SCP-SP-1-LCP_FW_ERR: System resetting module 4 to recover
    from error: Linecard received system exception
    00:27:15: %OIR-SP-3-PWRCYCLE: Card in module 4, is being power-cycled Off
    (Module Reset due to exception or user request)
    00:27:15: %C6KPWR-SP-4-DISABLED: power to module in slot 4 set Off (Module
    Reset due to exception or user request)
  ```

  Conditions:

  - CAT6500 switch or Cisco7600 that is running Cisco IOS Release 12.2(33)SRB1 or Release 12.2(33)SRB2.
  - This issue is NOT applicable for Cisco IOS 12.2(18)SXF releases.
  - Affected Modules: WS-X6704-10GE WS-X6748-GE-TX.

  Workaround: Use “test platform firmware component” to capture ASIC register values.

- 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.

- CSCsl55521

  Symptoms: Router may experience BGP convergence issues.

  Conditions: This problem has been seen when lot of aggregates are configured on a router.

  Workaround: Add all aggregates after router has fully converged.

- 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.

- CSCsl56824

  Symptoms: STP does not block a port and creates network loop after reload PE router.

  Conditions: This problem is observed when using VPLS.

  Workaround: There is no workaround.

- CSCsl60107

  Symptoms: VPLS/EoMPLS traffic may be dropped at imposition when a WRED policy applied to any port on the same HW datapath on SIP600 or ES20.

  Additionally, QoS may be incorrectly applied and traffic may stop on an FRR cutover of a VPLS/EoMPLS VC under similar conditions to above.

  Conditions:

  1. If a VPLS/EoMPLS VC egresses a port with no QoS applied and any other port on the LC has a WRED policy applied, the VC’s traffic may be dropped in the imposition direction, or misqueued.
  2. If a VC is FRR protected and BOTH the primary and backup paths egress ports on the second datapath on ES20 (ports 10-19), VC traffic may be dropped on tunnel switchover to the backup path.

  Workaround:

  1. Configure QoS on the egress interface carrying the VPLS/EoMPLS VC.
  2. Configure primary and backup tunnel paths to egress interfaces on the first 10 ports of ES20.

- CSCsl60761

  Symptoms: On reloading the router with scaled QoS configurations, the OSM LC may observe memory fragmentation errors.

  Conditions: QoS configurations should be scaled configs.

  Workaround: There is no workaround.

- CSCsl61225

  Symptoms: NSE150 is reloading due to a PXF crash on TMC1, Col 1, Row 2.

  Impact: Operation of the network since router is loading.

  Conditions: This symptom is seen on a router that is running Cisco IOS Release 12.2(31)SB8.

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

  Workaround: There is no workaround.

- CSCsl62346

  Symptoms: Class queue experiences unexpected high packet drops.

  Conditions: This symptom is noticed on Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRB image and later. When a service policy is applied on ATM PVC on SPA-2xOC3-ATM hosted by 7600-SIP-400, the packet drops are unusually high and throughput on the class queue is much less than the expected.

  Workaround: Configure WRED on the class queue by using the **random-detect aggregate** command. OR Increase the queue length of the **class using queue-limit** command, but this is inefficient use of buffers.

- CSCsl65407

  Symptoms: A routing loop was formed in MPLS/VPN network topology with EIGRP as the PE-CE routing protocol.

  Conditions: A receiving Provider Edge (PE) router does not update the EIGRP topology entry for a prefix to match the metric information advertised in the BGP ext.community attribute from the neighboring PE router. EIGRP is ignoring the metric information within the BGP ext. community attribute and opting to use the metric defined within the **redistribute bgp** *AS* **metric k1 k2 k3 k4 k5** command.

  Workaround: As a temporary solution, modify the **redistribute bgp** *AS* **metric k1 k2 k3 k4 k5 command to redistribute bgp** *AS* and then add a **default-metric k1 k2 k3 k4 k5** command. Clearing the routing table of the PE may also be necessary.

- CSCsl67817

  Symptoms: When you have lots of channels configured on chstm1/choc12 card, the ac mgr process on the standby would go high whenever there is a change in the link (UP/DOWN).

  Conditions: This symptom occurs during config loads and link flaps.

  Workaround: There is no workaround.

- CSCsl68031

  Symptoms: PPPoE sessions fail to come up.

  Conditions: This happens only when a RBE and PPPoE are configured on the same ATM subinterface.

  Workaround: Configure “no service pppoe-spoof-detect” to bring up a PPPoE session.

- CSCsl69838

  Symptoms: MPLS-TE Fast Reroute is failing upon switching from active to backup tunnel configured on SPA-5X1GE-V2 in SIP-400. The backup TE tunnel is activated as expected, but no traffic is sent on it.

  Conditions: This symptom occurs when MPLS-TE Fast Reroute node protection is configured using network interfaces on SIP-400.

  Workaround: The problem does not occur when the network interfaces are configured on SIP-600.

- CSCsl70343

  Symptoms: When Ethernet CFM is enabled and MEP is configured on the routers, it is not learning the remote MEPs.

  Conditions: Output is not seen when executing the **show ethernet cfm maintenance-points remote level 5** command.

  Workaround: There is no workaround.

- CSCsl70617

  Symptoms: User cannot use the redundant card once the router is reloaded with APS configuration.

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

  Workaround: Do a “no card” followed by “card” CLI for getting card back in functional state.

- CSCsl70667

  Symptoms: A line card crash is observed after the following error messages:

  ```
  FIBXDRINV: Invalid XDR format. FIB entry XDR has bogus routecount
  ```

  Conditions: This error message and crash are seen very rarely after OIR of the line card.

  Workaround: There is no workaround.

- CSCsl71254

  Symptoms: A Cisco 7609-S router, with RSP720 processor, using ES20 line card, and running Cisco IOS 12.2(33)SRB2 crashes

  Conditions: When configuring L3 subinterface with dot1Q NATIVE encapsulation on ES20 card interface, where already service-instance is configured, router crashes.

  Workaround: There is no workaround.

- CSCsl71540

  Symptoms: Router reloads when the **sh ip bgp** *options* command is entered.

  Conditions: This is seen in releases where CSCsj22187 is fixed.

  Workaround: There is no workaround.

- CSCsl72281

  Symptoms: After a Cisco 7600 series router reloads, host routes created by DHCP relay process for DHCP clients that are connected to unnumbered VLAN interfaces point to wrong VLAN interface.

  Conditions: This symptom occurs when interface-index value parameter on the router changes after the router reloads. This parameter is stored in DHCP bindings database on TFTP or FTP server. It is recalculated in case of the router reloading and may change if a new interface is added or existing interface is removed from the configuration. For example, a single interface VLAN is added to the configuration prior to the router reloading.

  Workaround: There is no workaround.

- CSCsl72636

  Symptoms: A Cisco router may experience traffic drop on frame-relay point-to- point subinterfaces during a SSO/NSF failover. This only occurs when a large number of frame-relay point-to-point interfaces are used.

  Conditions: This symptom is observed on a Cisco router that is running either Cisco IOS Release 12.2(33)SB or later releases, or Cisco IOS Release 12.2(33) SRB or later releases, that is configured for Stateful-Switchover (SSO) and Nonstop Forwarding (NSF).

  Workaround: There is no workaround.

- CSCsl72789

  Symptoms: SW_INIT_TIMEOUT message for ES20 line cards, line card may or may not recover.

  Conditions: Generally this error is seen with large routing tables, large configurations with many subinterfaces, or in the case of hardware failure.

  Workaround: Depending on the source of the error, the workaround may be to reload the line card or reload the chassis. Some problems may have no workaround.

  Further Problem Description: This fix will effectively remove the possibility of a SW_INIT_TIMEOUT.

- CSCsl74120

  Symptoms: Classification will be broken after OIR in OSMs as the OSM queues are not created.

  Conditions: This symptom is seen after OIR.

  Trigger: Queues are not created after OIR of LC or bootup OSM and FW. Issue seen only if OSM is configured.

  Impact: Impacts service policy classification done on the OSM queues.

  Workaround: Removing and attaching the policy again on the interface will solve the issue.

- CSCsl74441

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

  Conditions: This occurs when establishing PPPoE/L2TP sessions on Cisco 7300 routers. CSCsk38385 addresses this issue on Cisco 7200 routers.

  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.

- CSCsl77385

  Symptoms: Long delay of RF_PROG_ACTIVE event is observed on CAT6K.

  Conditions: This problem is seen with system bootup with scale configuration.

  Trigger: CAT6K MLS Multicast.

  Impact: This long delay caused AToM VCs to not be able to come up after a switchover.

  Workaround: There is no workaround.

- CSCsl77525

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

  Conditions: Standard PPPoEoA LNS session configurations. Passing traffic downstream and applying 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.

- CSCsl78159

  Symptoms: The **no passive-interface** command in OSPF configuration is not synchronized to standby RP. There are no errors reported.

  Conditions: The following sequence of OSPF configuration commands leads to the problem:

  1. **passive-interface default**
  2. **no passive-interface Serial2/0**
  3. **no passive-interface default**

  Workaround: Remove and restore OSPF process configuration.

  Further Problem Description: Here is an example of the difference in active and standby RP configuration:

```
ACTIVE RP:
router ospf 200 vrf test
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
 default-information originate metric 30 metric-type 1
!

STANDBY RP:
router ospf 200 vrf test
 log-adjacency-changes
 passive-interface default
 no passive-interface Serial2/0
 network 0.0.0.0 255.255.255.255 area 0
 default-information originate metric 30 metric-type 1
!
```

- CSCsl79195

  Symptoms: Following boot, or reload, of standby supervisor, the XDR_ISSUNEGOFAIL error message is seen relating to the standby SP. This can only be seen on a Cisco 6500/7600 as this is specific to the supervisor card.

  Conditions: This symptom is only seen if the standby supervisor is reloaded after it has first booted far enough for the XDR peers representing it to have been created on the active RP, but before the platform signals the OIR event for the card. A typical scenario is a transient RF progression failure.

  Workaround: Reload the standby supervisor.

- CSCsl82259

  Symptoms: When ATM AAL5 mode scalable AToM is configured on PE router and input traffic from CE uses AAL5 SNAP bridge encapsulation, traffic will be dropped by the LC.

  Conditions:

  1. Scalable AToM using AAL5 mode.
  2. Incoming traffic uses AAL5 SNAP bridge encapsulation.

  Workaround: Do not use AAL5SNAP encapsulation to configure PVC.

- CSCsl83415

  Symptoms: After executing the following CLI (steps mentioned alphabetically) via a script (not reproducible manually), the router sometimes crashes:

```
Test10 :
---------
a. clear ip bgp 10.0.101.46 ipv4 multicast out
b. clear ip bgp 10.0.101.47 ipv4 multicast out
Test 1:
-------
c. show ip bgp ipv4 multicast nei 10.0.101.2
d. show ip bgp ipv4 multicast [<prefix>]
e. config t
```

  Crash does not happen for each of the following cases:

  1. If same CLI is cut-paste manually, there is no crash.
  2. If **clear cli** is not executed, there is no crash.
  3. If **config term** is not entered, there is no crash.

  Conditions: The symptom occurs after executing the above CLI.

  Workaround: There is no workaround.

- CSCsl83479

  Symptoms: A router configured with BGP may crash when de-configuring VRFs through the CLI.

  Conditions: The crash is more likely to happen if a large number of VRFs are de-configured at the same time and the VPN table in BGP contains a large number of prefixes.

  Workaround: There is no workaround.

- CSCsl85847

  Symptoms: Router may reload due to some sup ipc issue. The XDR gets disabled with the line card and the RP-SP IPC communication is broken. External Data Representation (XDR) communication to a line card is disabled, followed by a message in this format:

```
%XDR-6-XDRDISABLEREQUEST: Peer in slot 2/0 (2) requested to be disabled due
 to: XDR Keepalive Timeout. Disabling linecard
```

  Conditions: This symptom is observed on Cisco 7600 series routers that are running Cisco IOS Release 12.2(33)SRB under some high XDR traffic conditions. Affected line card can be a SIP card, line card with DFC or SP.

  Workaround: There is no workaround.

Further Problem Description: Most common cause of high XDR traffic is flap of a routing peer with a high number of advertised prefixes. This will cause a high number of updates to the Forwarding Information Base (FIB), which has to be distributed to SIP cards, line cards with DFC and SP.

- CSCsl86206

  Symptoms: This problem is internal-only. It will not affect any functioning of the router.

  Conditions: User would need to have a queuing policy-map applied to an LNS session, then remove that policy-map and replace it with a non-queuing 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 failure to Session Manager. Session Manager finishes up cleaning up the session.

  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.

  Workaround: There is no workaround.

- CSCsl89425

  Symptoms: Bidirectional Forwarding Detection (BFD) sessions do not scale. This symptom is especially visible with OSPF client when one of the peers is rebooted after configuring maximum number of BFD sessions.

  Conditions: This symptom occurs when configuring maximum BFD sessions or total number of BFD sessions too close to maximum limit.

  Workaround: Configure 90% of maximum allowed BFD sessions.

- CSCsl93608

  Symptoms: Error messages are observed on the active console when the standby supervisor is booting up. This eventually leads to continuous reload of the standby supervisor.

  Conditions: It happens only when ISIS VRF is configured. Bulk-sync failure due to PRC mismatch.

  Issue Verification: The error can be seen by using the **show redundancy config-sync failures prc** command.

  Workaround: There is no workaround.

- CSCsl94259

  Symptoms: When applying the service policy on main interface, exceed error message is seen.

  Conditions: This symptom occurs when applying a policy or doing the OIR.

  Workaround: There is no workaround.

- CSCsl94499

  Symptoms: When applying the **mpls ip** under the top configuration mode command, the standby RP may be reset and the active RP generates the following error message:

  ```
  Dec 27 09:14:43.095 PST: %RTMGR-3-TOPO_SYNC_ERR: Failed to duplicate active topology
  on standby. (rc=15), id 1E000000 {default:ipv6:base}
  ```

Conditions: The problem happens on a Cisco 7600 series router when applying the **no mpls ip** top configuration mode command.

Workaround: Enable the IPv6 routing explicitly via the **ipv6 unicast- routing** command before issuing the **no mpls ip** command.

Further Problem Description: There is a synchronization (or timing) issue on IPv6 routing shutdown between active and standby RPs.

- CSCsl96417

  Symptoms: A router crashes.

  Conditions: On ISSU upgrade with ATM PVCs (configured with xconnect), the router crashes on running the **issu runversion** command. This is seen during the router upgrade with ATM ACs (configured with xconnect), configuration from rsp72043-adventerprisek9-mz.122-33.SRB2 to rsp72043-adventerprisek9-mz.122-32.8.11.SRC6 and in the issu runversion.

  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.

- 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.

- 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: The problem occurs when the router has a configuration greater than 0.5 Megabytes.

  Workaround: There is no workaround.

- 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.

- CSCsm13408

  Symptoms: DHCP renew packets are ignored after a redundancy forced switchover.

  Conditions: This is only present after a forced switch-over from Active to Standby RP, and only for VRF-transferred type of ip-sessions.

  Workaround: Prevent switch over, and or make your DHCP lease time long, like 24 hours.

- CSCsm13783

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

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

  Workaround: There is no workaround.

  Further Information: This is a regression bug, caused by CSCsl64889.

- CSCsm14007

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

  Conditions: This problem has been reported on a Cisco 10000 router that is running Cisco IOS Release 12.2(31)SB6.

  Trigger: Unknown.

  Impact: Monitoring/Troubleshooting of Virtual-access using SNMP is impacted.

  Workaround: There is no workaround.

Further Problem Description: Interface counters as seen in the output from “show interface” are incrementing OK ifInOctets and ifHCInOctets are incrementing. The problem is only affecting some Virtual Access Interfaces, not all.

- CSCsm16309

  Symptoms: Crash in BFD subsystem possible after last BFD session is removed.

  Conditions: When all the BFD sessions are removed and BFD process stops cleaning up all data structures.

  Workaround: There is no workaround.

- CSCsm19663

  Symptoms: Router crashes when MPLS VPN configurations are applied.

  Conditions: This symptom 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)#ex
72a(config-subif)#no shut
```

  Workaround: There is no workaround.

- CSCsm20102

  Symptoms: This issue results in a 0.4 to 2.5% of traffic loss.

  Conditions: Sending traffic at a rate of 70% across large number of MLPPP bundles with QoS and netflow configured results in traffic loss.

  Traffic rate is well below the cfg drop rate(s) of the applied QoS policy. PXF counters and policy-map counters show now drops.

  Reduced traffic rate to 40% saw the same issue.

  Workaround: Removing QoS policy or turning off netflow makes issue go away.

  Note: In both cases a write-mem/reload must be issued or cards must be reloaded via a “hw-module slot x reset” before changes take effect.

  Reducing number of MLPPP bundles, issue goes away.

  Further Problem Description: It affects distributed platforms (Cisco 10000 and others).

- CSCsm21728

  Symptoms: A router crashes when CPU_MONITOR between RP and SP messages have not been heard for more than 150 seconds. This is happening with a congested condition that is running on internal EOBC.

  Conditions: This symptom occurs when there are control data burst and congestions at internal EOBC.

  Workaround: There is no workaround.

- CSCsm23764

  Symptoms: Device keeps reloading every 50 minutes.

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

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

  Impact: This issue affects operations.

  Workaround: Reload active PRE if this issue occurs.

- CSCsm30581

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

  Conditions: This can happen during normal operation of the system 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 Cisco IOS Release 12.2(31)SB3 did not show this problem.

- CSCsm34469

  Symptoms: AFter PRE fails over to the standby, and then fails to the standby again, 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 have to be configured on the Cisco 10000 PRE-2

  1. Redundancy mode SSO.
  2. encapsulation PPP.
  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.

- CSCsm38142

  Symptoms: There is a potential memory leak on Cisco 7600 RP due to software defect in Cisco IOS Release 12.2(33)SRB.

  Conditions: It is observed if any QoS policy (service-policy command) is configured on router. It only impacts distributed platform such as Cisco 7600.

  Workaround: There is no workaround. Eventually the router could exhaust all available memory and impact router functionality.

- CSCsm39159

  Symptoms: ARP HA CPU tracebacks may be seen on the STANDBY PRE while it is booting up.

  Conditions: This symptom is seen under extreme cases of large ARP tables. The Cisco 10000 router could generate ARP HA tracebacks on the STANDBY PRE while it is booting up.

  Workaround: There is no workaround.

- CSCsm41685

  Symptoms: The ciscoEnhancedMemPoolMIB table is empty.

Conditions: The ciscoEnhancedMemPoolMIB table is empty with Cisco 7301 series router that is loaded with Cisco IOS Release 12.2(31)SB11 image.

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.

- 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: Cisco ISG reloads when subscriber sessions have Traffic Classes.

  Conditions: This behavior occurs when 1k-24k sessions go down and come up.

  Workaround: There is no workaround.

- CSCsm62033

  Symptoms: We mark the Call Serial Number AVP in the ICRP as mandatory. Other vendor implementation rejects it, and the l2tp session cannot come up.

  Workaround: There is no workaround.

- CSCsm62038

  Symptoms: A Cisco 7300 with NSE-100 crashes if you configure hierarchical policy-map with **set** command in the second level. Reason is that **set** command is NOT supported in the second level policy in the PXF.

  Workaround: Do not configure set in second level of hierarchical policy-map.

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

- CSCsm62533

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

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

  Workaround: There is no workaround.

- CSCsm65976

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

  Conditions: This occurs when the VRF is configured as peruser or service profile through the “ip:vrf-id ...” “ip:unnumbered ...” VSAs.

  Workaround: Use **lcp:interface-config=ip vrf forwarding** *vrf* **lcp:interface-config=ip unnumbered** *loopback interface*.

- 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 PRE-2 that is running an engineering special based on Cisco IOS Release 12.2(31)SB10 crashes and reloads due to a bus error.

  Conditions: The Cisco 10000 had the following number of users: pppoe - 4308 vpdn - 926.

  Workaround: There is no workaround.

- 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 (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 is seen on a Cisco 10000 that is running Cisco IOS Release 12.2(31)SB9 image. 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 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 second.

  Workaround: There is no workaround.

- CSCsm77558

  Symptoms: NODESTROYSUBBLOCK error message is seen when swidb is being reused, and these subblocks are still attached to the swidb.

  Conditions: Typically this will be seen in thrashing situations or whenever sessions are being disrupted.

  Workaround: There is no workaround.

- CSCsm78550

  Symptoms: Reassembly index is not allocated after flapping the bundles.

  Conditions: Configure MLPoLNS multi-member bundle.

  Workaround: The **clear vpdn tunnel l2tp all** or **clear ppp interface** commands will restore the bundle.

- CSCsm83777

  Symptoms: There is an address error crash running Cisco IOS Release 12.2(31)SB11. Decodes indicate Layer 4 redirect.

Conditions: Not known.

Workaround: There is no workaround.

- CSCsm86753

  Symptoms: Traceback is seen using redirection.

  Conditions: This symptom is seen when using redirection in ISG.

  Workaround: There is no workaround.

- CSCsm89620

  Symptoms: Billing fails for users.

  Conditions: AAA Accounting records are missing attr 8 for framed-ip-address only for stop records of a service profile. Here 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 attr
```

  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 the services.

- 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 see n when we enable time only prepaid service on the ISG.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(31)SB21

Cisco IOS Release 12.2(31)SB21 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)SB21 but may be open in previous Cisco IOS releases.

- CSCsk25046

  Symptoms: For a policy applied to an interface with an ifindex of 14, the corresponding entry will not appear in cbQosServicePolicyTable. This is impacting device monitoring.

  Conditions: This symptom occurs under the following conditions:

  - There should be an interface with an ifindex of 14 with a policy applied.
  - There should a be a policy applied on the control plane.

  Workaround: Remove the policy on the control plane.

- CSCsv08352

  Symptoms: Some static routes are not in the IP routing table state after a stateful switchover (SSO).

  Conditions: This only occurs following a SSO event.

Workaround: Perform a **shut/no shut** of interface if the route does not come up automatically.

- CSCsw24779

  Symptoms: A Cisco 7200 series router emits tracebacks.

  Conditions: This symptom is observed when a service policy with netflow sampler is attached to a PVC.

  Workaround: There is no workaround.

- CSCsz39222

  Symptoms: A Cisco router reloads and the crashinfo file indicates a cache error. CPO_ECC has the following value:

  ```
  Cache error detected! CPO_ECC (reg 26/0): 0xC0000000
  ```

  This is a hardware corrected cache error that should not result in a router reload.

  Conditions: This symptom is observed when register 26/0 contains 0xC0000000. This issue affects the RAN SVC card, NPE-G1 on a Cisco 7200 platform, NSE-150 on a Cisco 7300 platform, Sup32 for Cisco 6500/7600 platforms, SIP line cards for the Cisco 6500/7600, Cisco 67XX lan line cards for the Cisco 6500/7600 platforms, Cisco AS5400XM, Cisco UBR10K/PRE4 and other platforms using the same memory controller chip. Sup720 is not affected. NPE-G2 is not affected. NSE-100 is not affected. While rare, there is no specific trigger for this failure other than having a single bit parity error on the ECC memory.

  Workaround: There is no workaround. The router will reload and continue normal operation. The fix prevents a crash after a single bit parity error occurs on the ECC memory.

  Further Problem Description: This symptom does not cause a parity error or actually cause the crash. This symptom is just to add an error handler for the specific case of a single bit correctable parity error in the ECC memory. The crash results from the parity error itself. The following is an example of the beginning of a crashinfo collection for a hardware corrected cache error:

  ```
  Cache error detected!
      CPO_ECC (reg 26/0): 0xC0000000
      CPO_CACHERI (reg 27/0): 0x34001DE0
      CPO_CACHERD (reg 27/1): 0x10800580
      CPO_CCHEDPA (reg 27/3): 0x017B4580
  ```

- CSCtf71673

  Symptoms: A Cisco 10000 series router shows a PRE crash due to memory-corruption with block overrun.

  Conditions: This symptom occurs when the system is configured for PTA and L2TP access. The system is using a special based on Cisco IOS Release 12.2(34) SB4 during a pilot phase. Other systems in the same environment that are using a widely deployed special based on Cisco IOS Release 12.2(31)SB13 have not shown this so far.

  Workaround: There is no workaround.

- CSCti04754

  Symptoms: PPPoE sessions are stuck at attempting state forever.

  Conditions: This symptom is observed when sessions are triggered during SSO time, which get stuck at attempting state.

  Workaround: Clear attempting state sessions by the **clear** command from box.

- CSCtn31909

  Symptoms: On a Cisco 10k router running Cisco IOS Release 12.2(31)SB18 and configured for SSO, PPP information reported in the active PRE is correct, but the standby PRE has a number of users with 0.0.0.0 IP that are idle.

  Conditions: This symptom occurs with the following conditions:

  - Users are stuck in the LCP phase and waiting.
  - Information on the active PRE is correct and the user is working fine.

  In case of PRE switchover, those sessions will be stuck and they will require manual clearing.

  Workaround: Use the **clear ppp id** *id* command to clear the user's session on standby. On switchover, that user will need to reconnect again.

- CSCtn42029

  Symptoms: PXF CPU CEF memory leak at HW Mac rewrite component.

```
#sh pxf cpu cef memory
FP CEF/MFIB/TFIB XCM Type usage:
Type   Name   Col   Total   Alloc   Size   Start      End        BitMap    Error
...
  6    Mac    5     524279  383641   8     30800000   30C00000   CB394174   0     <===
HW Mac rewrite memory allocation level
...
C10K CEF/MFIB/TFIB PXF allocations:
Types      Alloc    Failed
Leaves     65598    0
Nodes      21205    0
Loadinfo   2047     0
Adjacency  87576    0
Rewrite    383642   0           <=== HW Mac rewrite allocated memory
```

  Conditions: This symptom is observed when lawful intercept taps are configured on the router.

  Workaround: Use the following workarounds:

  1. Switchover.
  2. Reload.
  3. Remove all LI taps.

- CSCtn86778

  Symptoms: When RBE-related configuration is present on the subinterface, encapsulation aal5auto PPP under an ATM VC is not allowed.

  Conditions: This symptom is observed when "atm route-bridged ip" is present on the ATM subinterface when trying to configure encapsulation aal5autoppp under the ATM VC.

  Workaround: Fix the encapsulation to snap when using RBE/PPPoE or mux when using PPPoA.

- CSCto77221

  Symptoms: Tracebacks eventually lead to a watchdog timeout crash.

  Conditions: This symptom is observed when a blocking call (process_wait_for_event via ppcp_accuquire_lock) is invoked from an interrupt context, where blocking calls are not allowed. Otherwise, watchdog timeout will kick in to crash the router if blocked too long. Disabling interrupts at atmdx_platform_modify_vc_policy is one such event leading to the crash.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(31)SB20

Cisco IOS Release 12.2(31)SB20 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)SB20 but may be open in previous Cisco IOS releases.

- CSCsb89847

  Symptoms: Source and destination Border Gateway Protocol (BGP) autonomous system (AS) information may not be properly updated.

  Conditions: This symptom is observed on a Cisco router that is configured for MSDP and NetFlow.

  Workaround: There is no workaround.

- CSCsl24511

  Symptoms: The problem was introduced due to the existence of multiple outgoing mcast interfaces. When ToS was changed from one interface during particle-based fastswitching, the change was carried to other interfaces, which made QoS policy perform incorrectly.

  Conditions: Fix should be applied to Cisco IOS Releases 12.2SR and 12.2SX. The reported issue is not seen haw_t, however, since it will fix CSCtj49957 which was duplicated to this DDTS, this fix should also be committed to t-train, and all other major branches which is NOT using MFIB forwarding.

  Workaround: Disable fastswitching and do process switching only.

- CSCsw77313

  Symptoms: After a successful login to a router, issuing the **login** command with a different username may result in the session appearing to execute with the new username even if the login attempt is unsuccessful. The new username will be reported by commands such as **show users** and it will be used in AAA processing and reporting. The privilege level of the new user is not changed. It stays at the privilege level of the original user.

  Conditions: The symptom is observed with authorization enabled with the **aaa authorization** configuration command.

  Workaround: Use “aaa authorization” to disable the **login** exec command.

- CSCsx11266

  Symptoms: Standby crashes after an SSO.

  Conditions: The symptom is observed with the following conditions:

  1. PVCs are discovered in 7600-1.
  2. Policy-map is attached to the PVCs (where ATM map is created).
  3. Traffic is sent from IXIA.
  4. After an SSO, the new active crashes.

  Workaround: There is no workaround.

- CSCtd10712

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCtd42810

  Symptoms: PPPoEoA sessions are not coming up because some VCs are in inactive state.

  Conditions: This symptom is observed when around 400 PVCs are configured with PPPoEoA sessions.

  Workaround: Save the configuration on the LAC, then reload the LAC.

- CSCth25634

  Symptoms: Password is prompted for twice for authentication.

  Conditions: This issue occurs when login authentication has the line password as fallback and RADIUS as primary. For example: aaa authentication login default group radius line.

  Workaround: Change the login authentication to fall back to the enable password that is configured on the UUT. For example: enable password <keyword> aaa authentication login default group radius enable.

  Further Information: The fix for this bug also fixes an unrelated problem that may allow unauthorized users access to EXEC mode if the “line” authentication method is configured with fallback to the “none” authentication method. In other words, if the following is configured:

  aaa new-model aaa authentication login MYMETHOD line none

  line con 0 login authentication MYMETHOD password <some password>

  then users providing the wrong password at the password prompt will be granted access.

  This issue was originally introduced by Cisco Bug ID CSCee85053, and fixed in some Cisco IOS releases via Cisco Bug IDs CSCsb26389 (“Failover for aaa authentication method LINE is broken”) and CSCsv06823 (“Authentication request doesnt failover to any method after enable”). However, the fix for this problem was not integrated into some Cisco IOS releases and this bug (CSCth25634) takes care of that.

  Note that Cisco Bug ID CSCti82605 (“AAA line password failed and access to switch still passed”) is a recent bug that was filed once it was determined that the fix for CSCee85053 was still missing from some Cisco IOS releases. CSCti82605 was then made a duplicate of this bug (CSCth25634) since the fix for this bug also fixes CSCti82605.

- CSCth69364

  Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.

  Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-dlsw.shtml.

- CSCti25339

  Symptoms: Cisco IOS device may experience a device reload.

  Conditions: This issue occurs when the Cisco IOS device is configured for SNMP and receives certain SNMP packets from an authenticated user. Successful exploitation causes the affected device to reload. This vulnerability could be exploited repeatedly to cause an extended DoS condition.

  Workaround: There is no workaround.

- CSCtj61284

  Symptoms: NAT overload does not work for non-directly connected destinations in MPLS-VPN configurations.

  Conditions: The symptom is observed with NAT overload configured to NAT traffic coming over an MPLS VPN to internet (via a VRF-enabled interface).

  Workaround: There is no workaround.

- CSCtj64807

  Symptoms: Router crashes while issuing the **show vlans dot1q internal** command.

  Conditions: The symptom is observed with the following conditions:

  1. One QinQ subinterface configured with inner VLAN as “any”.
  2. More than 32 QinQ subinterfaces configured with same outer VLAN.
  3. All subinterfaces are removed except subinterface configured with “any” inner VLAN.

  Workaround 1: For any Cisco 10000 series router which has had its first crash - on any subinterface if the outer VLAN has second-dot1q VLAN as only “any”, immediately delete the sub-interface and recreate it. Then add a dummy VLAN/sub-interface to this outer VLAN.

  Workaround 2: On any outer VLAN (in array state) if they have less than 5 inner VLANs, add a dummy VLAN/subinterface.

  Workaround 3: For any Cisco 10000 series router which has not had a crash but has subinterface/outer VLAN with second-dot1q VLAN as only “any” and active sessions, add a dummy VLAN/sub-interface to this outer (tree state) VLAN.

- CSCtj67572

  Symptoms: In an mVPN environment, an RR that is running Cisco IOS Release 12.2 (31)SB18 has update-group stuck in non-converged state, with no updates being sent to members of the group.

  Conditions: The symptom is observed when a member of the group activates the RR in MDT AF.

  Workaround: Clear the BGP session between the RR and a client that triggered the issue.

- CSCtj74542

  Symptoms: Router crashes.

  Conditions: The symptom is observed on a Cisco 10000 series router when you configure more than 33 QinQ subinterfaces all having the same outer VLAN and at least one of them has a second dot1q configured as “any”. Bring up a PPP session through the subinterface that has the second dot1q configured as “any”. Delete all other subinterfaces. Now try to clear the PPP session or delete the last subinterface.

  Workaround: There is no workaround.

- CSCtj87180

  Symptoms: An LAC router running VPDN may crash when it receives an invalid redirect from the peer with a CDN error message of “SSS Manager Disconnected Session”.

  Conditions: The symptom is observed when the LAC router receives an incorrect “Error code(9): Try another directed and Optional msg: SSS Manager disconnected session <<<< INVALID” from the multihop peer.

  Workaround: There is no workaround.

- CSCtk62453

  The Cisco 10000 Series Router is affected by a denial of service (DoS) vulnerability where an attacker could cause a device reload by sending a series of ICMP packets.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are also available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-c10k.shtml.

- CSCtn01821

  Symptoms: A crash can occur.

  Conditions: The symptom is observed when:

  1. You use the command **no ipv6 unicast-routing**.
  2. You then do a shut/no shut of the interface towards the PE.

  Workaround: Do not use **no ipv6 unicast-routing**. (Note: using this command is not a very common operation.)

Resolved Caveats—Cisco IOS Release 12.2(31)SB19

Cisco IOS Release 12.2(31)SB19 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)SB19 but may be open in previous Cisco IOS releases.

- CSCec51750

  Symptoms: A router that is configured for HTTP secure-server may reload unexpectedly because of an internal memory corruption.

  Conditions: IOS HTTP Secure server enabled.

  Workaround: Disable HTTPS with the **no ip http secure-server** command.

- CSCek10384

  Symptoms: A Cisco 7200 router that is performing NAT could drop IPSec packets.

  Conditions: This symptom is observed on a Cisco 7200 router that is performing NAT functionality for IPSec transit packets. The router will NAT and forward the Inside to Outside IPSec (ESP) packets, but might drop the return IPSec packets from Outside to Inside.

  Workaround: Disable NAT for IPSec.

- CSCse26921

  Symptoms: After configuring a new route-target export under the IP VRF definition, the BGP routes may not get updated with the new route-target.

  Conditions: The symptom is observed under the following conditions:

  - Cisco IOS 12.4 releases.
  - It is not seen in Cisco IOS Releases 12.0S or 12.2S.
  - It is platform independent. That is it can be observed on all platforms that are running a Cisco IOS Release 12.4.

  Workaround: Using the following command: **clear ip route vrf** *name prefix* will cause the route to be correctly updated.

- CSCta33011

  Symptoms: You may not be able to terminate PPPoE sessions on a Cisco ASR P2. The issue starts after days of normal working operation.

  Conditions: The symptom is observed on a Cisco ASR RP2 configured as an LNS.

  Workaround: There is no workaround.

  Further Problem Description: Except PPP sessions, other functionality works fine. Only PPP is in a stuck state and reload is the only option to recover from this state.

- CSCtd30544

  Symptoms: NetFlow is showing Null in the destination interface even though packets are not getting dropped or blocked.

  Conditions: This symptom is seen when connected to the LNS via VPDN and browsing HTTP. Intermittently Null output is seen as the destination interface as the packet being punted between different CEF switching paths due to **ip tcp adjust-mss** *value* configuration that is applied on the destination interface.

  Workaround: Remove **ip tcp adjust-mss** *value* from the destination interface.

- CSCtd62220

  Symptoms: The following error is seen:

  ```
  %DATACORRUPTION-1-DATAINCONSISTENCY: copy error
  ```

  Conditions: The symptom is observed under normal use. The issue is not consistently reproducible and is a corner case.

  Workaround: There is no workaround.

- CSCte49283

  Symptoms: Sometimes the LNS router sends an incorrect NAS-Port value.

  Conditions: The symptom is observed when the LNS router sends a stop accounting-request to the RADIUS server.

  Workaround: There is no workaround.

- CSCte98052

  Symptoms: Shaping values may result in stuck MQC queues during times of heavy traffic. The fail signature will present as a unidirectional transmit problem and the command **show policy-map interface** may report:

  ```
  Router#sh policy-map int a4/0.16 | i no-buffer drops
  (queue depth/total drops/no-buffer drops) 195/44432/0
  (queue depth/total drops/no-buffer drops) 0/15036/0
  (queue depth/total drops/no-buffer drops) 64/14962/0
  (queue depth/total drops/no-buffer drops) 64/29470/0 (shows all packets dropped)
  ```

  Conditions: The symptom is observed on a Cisco 7304/NPE-G100/PA-CC/PA-A3-T3 that is running Cisco IOS Release 12.2(33)SB7 and deploying a scaled PVC configuration (600+) with relatively low ATM traffic.

  Workaround 1: Remove “service-policy output” from PVC.

  This is a preventative workaround but results in loss of functionality.

  Workaround 2: Perform a **shut** followed by a **no shut** on the affected subinterface.

  This is a recovery workaround which requires manual intervention.

- CSCtf71636

  Symptoms: The router crashes while configuring/unconfiguring random detect.

Conditions: The symptom is observed with Cisco IOS interim Release 12.2 (31.17.01)SB. The policy given below has to be applied on FR DLCI interface for this issue to occur:

```
Policy Map output-policy
Class prec2
bandwidth 460 (kbps)
Class prec4
bandwidth 460 (kbps)
```

Next, the following command sequence causes the router to crash:

config terminal

policy-map output-policy

class class-default

fair-queue

random-detect

no fair-queue

random-detect

no random-detect

random-detect

Workaround: There is no workaround.

- CSCtf77047

  Symptoms: Ping ATM subinterface peer IP address has packet loss from Cisco 7206.

  Conditions: This symptom occurs with the following:

  1. NPE-G2+PA-MC-STM-1SMI+PA-A6-OC3SML
  2. Enable EIGRP on ATM subinterface

  Workaround: There is no workaround.

- CSCtg31434

  Symptoms: A Cisco router crashes due to an unexpected exception to the CPU.

  Conditions: This symptom occurs when the **privilege interface level 10 ppp authentication** command is entered. This symptom is observed in Cisco IOS Release 12.2(31)SB through Release 12.2(31)SB18, and in Cisco IOS Releases 12.2(33)SB and 12.2(34)SB.

  Workaround: There is no workaround.

- CSCth83055

  Symptoms: VPNv4 route-reflector with 240K from multiple neighbors crashes in certain conditions.

  Conditions: The symptom is observed with Cisco IOS Release 12.2(31)SB16.

  Workaround: There is no workaround.

  Further Problem Description: The issue is due to heavy BGP churn in the network. The PEs become desynchronized with the RRs.

- CSCti97810

  Symptoms: A “%SYS-2-FREEBAD” memory traceback is seen on an HA router.

  Conditions: The symptom is observed on an HA router approximately 3-4 minutes after loading the image on an HA router.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(31)SB18

Cisco IOS Release 12.2(31)SB18 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)SB18 but may be open in previous Cisco IOS releases.

- CSCek78386

  Symptoms: A Cisco 7300 series router crashes when xconnect (AToM) is configured on the ATM (PA-A6) interface and when you wait for the VC to come up by issuing the **show mpls l2transport vc** command.

  Conditions: The symptom is observed after configuring VC mode with both AAL5 and AAL0 and when checking for the AToM circuit to come up.

  Workaround: There is no workaround.

- CSCsb37698

  Symptoms: When you configure NAT, an IPv6 configuration is evoked unintentionally in addition to the NAT configuration.

  Conditions: This symptom is observed when you enter the **ip nat pool** *name* **192.168.22.100 192.168.22.120 netmask 255.255.255.0** command. When you do so, the output of the **show running-config** command shows the above-mentioned command and, in addition and unexpectedly, also the **ipv6 nat v6v4 pool** *name* **192.168.22.100 192.168.22.120 netmask 255.255.255.0** command.

  Workaround: There is no workaround.

- CSCsc13670

  Symptoms: The backup configurations that are generated by the Archive feature may be truncated.

  Conditions: This symptom is observed when you reload the router with the Archive feature enabled.

  Workaround: Enter the privileged mode.

- CSCsc91697

  Symptoms: DBS-applied values do not get dynamically synchronized to the Standby.

  Conditions: The symptom is observed with DBS-applied values (such as PCR, SCR, and MBS).

  Workaround: There is no workaround.

- CSCsd99763

  Symptoms: A Cisco 7200 series router reloads unexpectedly while configuring BGP access list.

  Conditions: This symptom is observed on a Cisco 7206VXR (NPE-G1) processor (revision A). The following commands serve as an example that causes router to reload unexpectedly:

```
config t
router bgp 100
neighbor EXTERNAL route-map MAP3 out
address-family ipv4 multicast
neighbor EXTERNAL route-map MAP3 out
!
ip as-path access-list 1 deny ^$
ip as-path access-list 2 permit ^(700)+(_1123)|_2374$|^(_700)+(_2374)+
(_1123)+$
```

```
ip as-path access-list 3 permit _3400_
ip as-path access-list 4 permit ^(700)+(_3400)|_1123$|^700$|_23\[0-9\]$
!
route-map MAP3 permit 10
match as-path 1
!
route-map MAP3 deny 20
match as-path 2
!
route-map MAP3 permit 30
match as-path 3
!
route-map MAP3 permit 40
match as-path 4
set metric 300
end
```

Workaround: There is no workaround.

- CSCsk35688

  Symptoms: Aggregate routes are not processed if all aggregated child routes are deleted prematurely.

  Conditions: The symptom is observed when all aggregated child routes are marked for deletion and the periodic function which processes the routes to be deleted deletes the route before the aggregate processing function gets a chance to process them and the aggregate route to which they belong.

  Workaround: Configuring “bgp aggregate-timer” to 0 or the lowest value would considerably reduce the chances of hitting this problem. In case this problem does occur, in order to delete the stale aggregate route, configure a temporary local BGP route (say, redistribute a static route or network a loopback) with its address being a subnet of the stale aggregate address and then remove the aggregate address and the added route. This should delete the route from table and send withdraws to the other routes also.

  Further Problem Description: The periodic function is by default called at 60 second intervals. The aggregate processing is normally done based on the CPU load. If there is no CPU load, then the aggregate processing function would be triggered within one second. As the CPU load increases, this function call will be triggered at higher intervals and if the CPU load is very high it could go as high as the maximum aggregate timer value configured via command. By default this maximum value is 30 seconds and is configurable with a range of 6-60 seconds and in some trains 0. So, if default values are configured, then as the CPU load increases, the chances of hitting this defect is higher.

- CSCsu76354

  Symptoms: Some ATM subinterfaces stop the output of packets after an SSO.

  Conditions: Though the encapsulation string is displayed and the VCCI value is not 0x0 on the normal sub-interfaces (using the by **show ip cef** *VRF IP* **plat** command) no encapsulation string is displayed and the VCCI value is 0x0 on the defective sub-interface after the SSO by the **show** command: Encap String:

After **shut/no shut** on the defective subinterface, the encapsulation string comes to be displayed and VCCI value is not 0x0 on it by the **show** command. Encap String: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

The incidence of this occurring is about one in every five SSO executions.

Workaround: There is no workaround.

- CSCsw73196

  Symptoms: BGP MDT session flaps when a router running Cisco IOS is interoperating with a router running Cisco IOS-XR and when withdrawal messages are sent by IOS to XR of previously advertised MDT prefixes.

  Conditions: MDT prefixes need to be exchanged by IOS and XR routers. If a withdrawal message is exchanged subsequently for any reason then this problem is seen.

  Workaround: There is no workaround.

- CSCsx27496

  Symptoms: Router may crash with an address error in the BGP function.

  Conditions: The symptom is observed when the router is configured for BGP and traffic is passing.

  Workaround: There is no workaround.

- CSCsy47987

  Symptoms: After an RP switchover occurs, some PPP interfaces remain up/down until the router is reloaded or the encapsulation is changed to HDLC.

  Conditions: The symptom is observed on a Cisco 10000 series router with dual PREs when some PPP interfaces are up and some are down after a PRE switchover. In addition, the “interface resets” counter on the problematic interface will increment.

  Workaround: Change the encapsulation to HDLC or try issuing the command **clear ppp interface**.

- CSCsy61367

  Symptoms: A router crashes when removing the VPN service from the PVC.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS interim Release 12.2(33.01.23)MCP04.

  Workaround: Do not enable VPN service for PTA service.

- CSCsz45567

  A device running Cisco IOS Software, Cisco IOS XE Software, or Cisco IOS XR Software is vulnerable to a remote denial of service condition if it is configured for Multiprotocol Label Switching (MPLS) and has support for Label Distribution Protocol (LDP).

  A crafted LDP UDP packet can cause an affected device running Cisco IOS Software or Cisco IOS XE Software to reload. On devices running affected versions of Cisco IOS XR Software, such packets can cause the device to restart the mpls_ldp process.

  A system is vulnerable if configured with either LDP or Tag Distribution Protocol (TDP).

  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-20100324-ldp.shtml

- CSCsz71787

  Symptoms: A router crashes when it is configured with DLSw.

Conditions: A vulnerability exists in Cisco IOS software when processing UDP and IP protocol 91 packets. This vulnerability does not affect TCP packet processing. A successful exploitation may result in a reload of the system, leading to a denial of service (DoS) condition.

Cisco IOS devices that are configured for DLSw with the **dlsw local- peer** automatically listen for IP protocol 91 packets. A Cisco IOS device that is configured for DLSw with the **dlsw local-peer peer-id** *IP- address* command listen for IP protocol 91 packets and UDP port 2067.

Cisco IOS devices listen to IP protocol 91 packets when DLSw is configured. However, it is only used if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

dlsw remote-peer 0 fst *ip-address*

It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the device from receiving and processing incoming UDP packets.

Workaround: The workaround consists of filtering UDP packets to port 2067 and IP protocol 91 packets. Filters can be applied at network boundaries to filter all IP protocol 91 packets and UDP packets to port 2067, or filters can be applied on individual affected devices to permit such traffic only from trusted peer IP addresses. However, since both of the protocols are connectionless, it is possible for an attacker to spoof malformed packets from legitimate peer IP addresses.

As soon as DLSw is configured, the Cisco IOS device begins listening on IP protocol 91. However, this protocol is used only if DLSw is configured for Fast Sequenced Transport (FST). A DLSw FST peer configuration will contain the following line:

dlsw remote-peer 0 fst *ip-address*

If FST is used, filtering IP protocol 91 will break the operation, so filters need to permit protocol 91 traffic from legitimate peer IP addresses.

It is possible to disable UDP processing in DLSw with the **dlsw udp-disable** command. However, disabling UDP only prevents the sending of UDP packets; it does not prevent the receiving and processing of incoming UDP packets. To protect a vulnerable device from malicious packets via UDP port 2067, both of the following actions must be taken:

1. Disable UDP outgoing packets with the **dlsw udp-disable** command.
2. Filter UDP 2067 in the vulnerable device using infrastructure ACL.

* Using Control Plane Policing on Affected Devices

Control Plane Policing (CoPP) can be used to block untrusted DLSw traffic to the device. Cisco IOS software releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP may be configured on a device to protect the management and control planes to minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic sent to infrastructure devices in accordance with existing security policies and configurations. The following example, which uses 192.168.100.1 to represent a trusted host, can be adapted to your network. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsw udp-disable** command, UDP port 2067 may also be completely filtered.

```
!--- Deny DLSw traffic from trusted hosts to all IP addresses
    !--- configured on all interfaces of the affected device so that
    !--- it will be allowed by the CoPP feature.

    access-list 111 deny udp host 192.168.100.1 any eq 2067
    access-list 111 deny 91 host 192.168.100.1 any
```

```
!--- Permit all other DLSw traffic sent to all IP addresses
!--- configured on all interfaces of the affected device so that it
!--- will be policed and dropped by the CoPP feature.

access-list 111 permit udp any any eq 2067
access-list 111 permit 91 any any

!--- Permit (Police or Drop)/Deny (Allow) all other Layer 3 and Layer 4
!--- traffic in accordance with existing security policies and
!--- configurations for traffic that is authorized to be sent
!--- to infrastructure devices.
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature.

class-map match-all drop-DLSw-class
 match access-group 111

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.

policy-map drop-DLSw-traffic
 class drop-DLSw-class
  drop

!--- Apply the Policy-Map to the Control-Plane of the
!--- device.

control-plane
 service-policy input drop-DLSw-traffic
```

In the above CoPP example, the access control entries (ACEs) that match the potential exploit packets with the “permit” action result in these packets being discarded by the policy-map “drop” function, while packets that match the “deny” action (not shown) are not affected by the policy-map drop function. Please note that in the Cisco IOS 12.2S and 12.0S trains, the policy-map syntax is different:

```
policy-map drop-DLSw-traffic
     class drop-DLSw-class
      police 32000 1500 1500 conform-action drop exceed-action drop
```

Additional information on the configuration and use of the CoPP feature is available at:

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd804fa16a.html

http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

* Using Infrastructure ACLs at Network Boundary

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and block that traffic at the border of your network. iACLs are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example shown below should be included as part of the deployed infrastructure access-list that will protect all devices with IP addresses in the infrastructure IP address range. If FST is not used, protocol 91 may be completely filtered. Additionally, if UDP is disabled with the **dlsw udp-disable** command, UDP port 2067 may also be completely filtered.

```
!--- Permit DLSw (UDP port 2067 and IP protocol 91) packets
    !--- from trusted hosts destined to infrastructure addresses.

    access-list 150 permit udp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES
MASK eq 2067
    access-list 150 permit 91 TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES
MASK

    !--- Deny DLSw (UDP port 2067 and IP protocol 91) packets from
    !--- all other sources destined to infrastructure addresses.

    access-list 150 deny udp any INFRASTRUCTURE_ADDRESSES MASK eq 2067
    access-list 150 deny 91 any INFRASTRUCTURE_ADDRESSES MASK

    !--- Permit/deny all other Layer 3 and Layer 4 traffic in accordance
    !--- with existing security policies and configurations.
    !--- Permit all other traffic to transit the device.

    access-list 150 permit ip any any

    interface serial 2/0
     ip access-group 150 in
```

The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

Further Problem Description: This vulnerability occurs on multiple events to be exploited. It is medium complexity in order to exploit and has never been seen in customers environment.

- CSCsz72591

  Symptoms: A router crashes with an Address Error (load or instruction fetch) exception.

  Conditions: The router must be configured to act as a DHCP client.

  Workaround: There is no workaround.

- CSCta18596

  Symptoms: The following tracebacks and messages appear on the console logs:

```
%ALIGN-3-SPURIOUS: Spurious memory access made at 0x61AB0C78 reading 0x22
%ALIGN-3-TRACE:
-Traceback= 61AB0C78 623849E8 62384A58 607CCD8C 61372428 613769FC 61376E68 613773C4
```

In addition, you may see instability of the serial interfaces (i.e.: when an interface is configured, it stays up for a while and then goes down).

Conditions: The symptoms are observed when upgrading to Cisco IOS Release 12.2(31)SB14 on a Cisco 7200 series router only on the interfaces configured with frame-relay fragmentation configured on the main interface.

Workaround 1: Use fragmentation in the map-class with FRTS (i.e.: configure “frame-relay traffic-shaping” under the main interface and configure fragmentation under the map-class and apply the map-class to PVC). For example:

```
interface Serial1/0.1/1/4/2:0
 no ip address
 encapsulation frame-relay IETF
         ...
 frame-relay traffic-shaping
 frame-relay lmi-type ansi
 frame-relay intf-type dce
 no clns route-cache
 max-reserved-bandwidth 100
!
interface Serial1/0.1/1/4/2:0.101 point-to-point
         ...
 frame-relay interface-dlci 101
  class BANKOFIRE-S1/0.1/1/4/2:0.101-SR611638725

map-class frame-relay BANKOFIRE-S1/0.1/1/4/2:0.101-SR611638725
 frame-relay cir 768000
 frame-relay mincir 768000
 no frame-relay adaptive-shaping
 service-policy input BANKOFIRE-IN-S1/0.1/1/4/2:0
 service-policy output BANKOFIRE-OUT-S1/0.1/1/4/2:0
 frame-relay fragment 600
!
```

Workaround 2: Make sure that the fragmentation size is different in different interfaces (with interface fragmentation).

- CSCtb59288

  Symptoms: A router crashes on ATM hw-module reset.

  Conditions: The crash happens when the ATM interface is OIRed.

  Workaround: There is no workaround.

- CSCtc48125

  Symptoms: Duplicated ARP entry when enabling ISG. When you enable ISG for the existing DHCP users, you may see the following:

```
GPKC10ki01#sh arp | i aaaa.bbbb.cccc
Internet  x.x.x.x          -   aaaa.bbbb.cccc  ARPA   GigabitEthernet1/0/2.1203
Internet  y.y.y.y         16   aaaa.bbbb.cccc  ARPA   GigabitEthernet1/0/2.1203
```

```
GPKC10ki01#
```

(The one without the age is the ISG user and the one with an age is the DHCP learned address.)

Conditions: The symptom is observed on a Cisco 10000 series router when enabling ISG on existing DHCP users.

Workaround: Disable multiple DHCP servers. Use one DHCP server.

- CSCtc84758

  Symptoms: On a router configured for ISG that is running postpaid Web-Logon users with SESM as the external portal, a memory leak may occur in RADIUS LOCAL SERVER.

  Conditions: The symptom is observed on a Cisco 10000 series router with a PRE-3 and running Cisco IOS Release 12.2(33)SB7 using SESM as a captive portal. The issue can be triggered with this sequence of events:

  1. Postpaid user is redirected to SESM.
  2. SESM sends Access-Request to router after captivating user/pass from postpaid user.
  3. RADIUS LOCAL SERVER creates AAA request and sends it to ISG.
  4. ISG creates another AAA request to send an Access-Request to authenticate the postpaid user.
  5. AAA receives a response from external AAA.
  6. AAA passes the response to RADIUS LOCAL SERVER which transmits an Access-Accept or Access-Reject to SESM.

  If the processing delay of sum (C,D,E,F) is greater than the SESM timeout, SESM will send another Access-Request with the same credentials for the Account logon postpaid user in B.

  If this occurs, policy/AAA will now use this second Account-Logon request from SESM for this user's Account Login and the policy will not free the AAA request from the former Account Logon request, hence the memory leak will present as RADIUS LOCAL SERVER.

  Workaround:

  1. Make sure SESM Account Logon Timeout > RADIUS timeout.
  2. Decrease load on external AAA (RADIUS) machines.

- CSCtc90779

  Symptoms: A router may crash after displaying align fatal errors pointing to PPPoE functions.

  Conditions: The symptom is observed on a Cisco 7206VXR router (NPE-G1) that is running Cisco IOS Release 12.2(31)SB15.

  Workaround: There is no workaround.

- CSCtd03798

  Symptoms: In an MPLS VPN, when a Cisco 7300 series router is being used as a PE, some prefixes lose reachability. The packet capture between PE and CE shows that the header checksum is incorrect:

  Protocol: ICMP (0x01) Header checksum: 0x93a8 (should be 0x9308)

  Conditions: The symptom is observed under the following conditions:

  - An MPLS VPN where a Cisco 7300 series router is being used as PE with NSE-100.
  - Both ingress and egress interfaces must be link ethernet interface (SPA/PA gigE or FE).
  - Egress interface towards CE must contain QoS marking and it should be a dot1q interface.

Workaround: Remove QoS marking.

Alternate workaround: Use Native GigE.

- CSCtd75033

  Symptoms: Cisco IOS Software is affected by NTP mode 7 denial-of-service vulnerability.

  Conditions: Cisco IOS Software with support for Network Time Protocol (NTP) contains a vulnerability processing specific NTP Control Mode 7 packets. This results in increased CPU on the device and increased traffic on the network segments.

  This is the same as the vulnerability which is described in http://www.kb.cert.org/vuls/id/568372.

  Cisco has release a public facing vulnerability alert at the following link:

  http://tools.cisco.com/security/center/viewAlert.x?alertId=19540

  Cisco IOS Software that has support for NTPv4 is NOT affected. NTPv4 was introduced into Cisco IOS Software: 12.4(15)XZ, 12.4(20)MR, 12.4(20)T, 12.4(20)YA, 12.4(22)GC1, 12.4(22)MD, 12.4(22)YB, 12.4(22)YD, 12.4(22)YE and 15.0(1)M.

  All other versions of Cisco IOS and Cisco IOS XE Software are affected.

  To see if a device is configured with NTP, log into the device and issue the CLI command **show running-config | include ntp**. If the output returns either of the following commands listed then the device is vulnerable:

```
ntp master <any following commands>
ntp peer <any following commands>
ntp server <any following commands>
ntp broadcast client
ntp multicast client
```

  The following example identifies a Cisco device that is configured with NTP:

```
router#show running-config | include ntp
      ntp peer 192.168.0.12
```

  The following example identifies a Cisco device that is not configured with NTP:

```
router#show running-config | include ntp
      router#
```

  To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the show version command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the show version command or may provide different output.

  The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router#show version
 Cisco Internetwork Operating System Software
 IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26), RELEASE SOFTWARE
```

```
(fc2)
       Technical Support: http://www.cisco.com/techsupport
       Copyright ) 1986-2008 by cisco Systems, Inc.
       Compiled Mon 17-Mar-08 14:39 by dchih

       <output truncated>
```

The following example shows a product that is running Cisco IOS Software Release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```
     Router#show version
     Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M), Version
 12.4(20)T, RELEASE SOFTWARE (fc3)
     Technical Support: http://www.cisco.com/techsupport
     Copyright ) 1986-2008 by Cisco Systems, Inc.
     Compiled Thu 10-Jul-08 20:25 by prod_rel_team

     <output truncated>
```

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide" at the following link:

http://www.cisco.com/warp/public/620/1.html

Workaround: There are no workarounds other than disabling NTP on the device. The following mitigations have been identified for this vulnerability; only packets destined for any configured IP address on the device can exploit this vulnerability. Transit traffic will not exploit this vulnerability.

Note: NTP peer authentication is not a workaround and is still a vulnerable configuration.

* NTP Access Group

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat access control lists (ACLs) that permit communication to these ports from trusted IP addresses. Unicast Reverse Path Forwarding (Unicast RPF) should be considered to be used in conjunction to offer a better mitigation solution.

```
     !--- Configure trusted peers for allowed access

     access-list 1 permit 171.70.173.55

     !--- Apply ACE to the NTP configuration

     ntp access-group peer 1
```

For additional information on NTP access control groups, consult the document titled "Performing Basic System Management" at the following link:

http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_basic_sys_manage.html#wp1034942

* Infrastructure Access Control Lists

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender's IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Although it is often difficult to block traffic that transits a network, it is possible to identify traffic that should never be allowed to target infrastructure devices and block that traffic at the border of networks.

Infrastructure ACLs (iACLs) are a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The iACL example below should be included as part of the deployed infrastructure access-list, which will help protect all devices with IP addresses in the infrastructure IP address range:

```
!---
!--- Feature: Network Time Protocol (NTP)
!---

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 123

!--- Note: If the router is acting as a NTP broadcast client
!---   via the interface command "ntp broadcast client"
!---   then broadcast and directed broadcasts must be
!---   filtered as well.  The following example covers
!---   an infrastructure address space of 192.168.0.X

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 192.168.0.255 eq ntp
access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 255.255.255.255 eq ntp

!--- Note: If the router is acting as a NTP multicast client
!---   via the interface command "ntp multicast client"
!---   then multicast IP packets to the mutlicast group must
!---   be filtered as well.  The following example covers
!---   a NTP multicast group of 239.0.0.1 (Default is
!---   224.0.1.1)

access-list 150 permit udp TRUSTED_SOURCE_ADDRESSES WILDCARD
    host 239.0.0.1 eq ntp

!--- Deny NTP traffic from all other sources destined
!--- to infrastructure addresses.

access-list 150 deny udp any
    INFRASTRUCTURE_ADDRESSES WILDCARD eq 123
```

```
!--- Permit/deny all other Layer 3 and Layer 4 traffic in
!--- accordance with existing security policies and
!--- configurations.  Permit all other traffic to transit the
!--- device.

access-list 150 permit ip any any

!--- Apply access-list to all interfaces (only one example
!--- shown)

interface fastEthernet 2/0
 ip access-group 150 in
```

The white paper entitled “Protecting Your Core: Infrastructure Protection Access Control Lists” presents guidelines and recommended deployment techniques for infrastructure protection access lists and is available at the following link:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801a1a55.shtml

* Control Plane Policing

Provided under Control Plane Policing there are two examples. The first aims at preventing the injection of malicious traffic from untrusted sources, whilst the second looks at rate limiting NTP traffic to the box.

- Filtering untrusted sources to the device.

Warning: Because the feature in this vulnerability utilizes UDP as a transport, it is possible to spoof the sender’s IP address, which may defeat ACLs that permit communication to these ports from trusted IP addresses. Unicast RPF should be considered to be used in conjunction to offer a better mitigation solution.

Control Plane Policing (CoPP) can be used to block untrusted UDP traffic to the device. Cisco IOS Software Releases 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T support the CoPP feature. CoPP can be configured on a device to help protect the management and control planes and minimize the risk and effectiveness of direct infrastructure attacks by explicitly permitting only authorized traffic that is sent to infrastructure devices in accordance with existing security policies and configurations. The CoPP example below should be included as part of the deployed CoPP, which will help protect all devices with IP addresses in the infrastructure IP address range.

```
!--- Feature: Network Time Protocol (NTP)

access-list 150 deny udp TRUSTED_SOURCE_ADDRESSES WILDCARD
     any eq 123

!--- Deny NTP traffic from all other sources destined
!--- to the device control plane.

access-list 150 permit udp any any eq 123

!--- Permit (Police or Drop)/Deny (Allow) all other Layer3 and
```

```
!--- Layer4 traffic in accordance with existing security policies
!--- and configurations for traffic that is authorized to be sent
!--- to infrastructure devices
!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all drop-udp-class
 match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.

policy-map drop-udp-traffic
 class drop-udp-class
  drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
 service-policy input drop-udp-traffic
```

In the above CoPP example, the access control list entries (ACEs) that match the potential exploit packets with the “permit” action result in these packets being discarded by the policy-map “drop” function, while packets that match the “deny” action (not shown) are not affected by the policy-map drop function.

- Rate Limiting the traffic to the device The CoPP example below could be included as part of the deployed CoPP, which will help protect targeted devices from processing large amounts of NTP traffic.

Warning: If the rate-limits are exceeded valid NTP traffic may also be dropped.

```
!--- Feature: Network Time Protocol (NTP)

access-list 150 permit udp any any eq 123

!--- Create a Class-Map for traffic to be policed by
!--- the CoPP feature

class-map match-all rate-udp-class
 match access-group 150

!--- Create a Policy-Map that will be applied to the
!--- Control-Plane of the device.
!--- NOTE: See section "4. Tuning the CoPP Policy" of
!--- http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html#5
!--- for more information on choosing the most
```

```
!--- appropriate traffic rates

policy-map rate-udp-traffic
 class rate-udp-class
  police 10000 1500 1500 conform-action transmit
        exceed-action drop violate-action drop

!--- Apply the Policy-Map to the
!--- Control-Plane of the device

control-plane
 service-policy input drop-udp-traffic
```

Additional information on the configuration and use of the CoPP feature can be found in the documents, “Control Plane Policing Implementation Best Practices” and “Cisco IOS Software Releases 12.2 S - Control Plane Policing” at the following links:

http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html and
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gtrtlimt.html

- CSCte10706

  Symptoms: When you configure FRF.12 “frame-relay fragment 512 end-to-end” on the serial interface, the router crashes.

  Conditions: The symptom is observed when you configure FRF.12 “frame-relay fragment 512 end-to-end” on a CJ-PA.

  Workaround: There is no workaround.

- CSCte42714

  Symptoms: A Cisco 7304 router crashes continuously after a reload.

  Conditions: The symptom is observed when the router is configured with an mGRE tunnel. Once the tunnel is configured, if the router is reloaded it starts crashing continuously.

  Workaround: Use point-to-point GRE tunnels.

- CSCte64313

  Symptoms: When BGP sessions flap and there is sufficient churn in the network, the RR may not send withdraws or advertisements for prefixes because of stale check-pointing left behind by the peer in the update-group that flapped.

  Conditions: The symptom is observed when the BGP session flaps and there is sufficiently large churn in the network. It is seen with Cisco IOS Release 12.2(31)SB17 and later. This release has the refresh update-group functionality introduced by CSCsl75177 in Cisco IOS Release 12.2(31)SB14, and CSCtb56083 committed in Cisco IOS Release 12.2(31)SB17, which brought in new update-group check-pointing code to resume update-generation after the BGP update-generation process suspends.

  Workaround: If there are missing routes (advertisements) on the receiving PE, the problem can be remedied by using the **clear ip bgp * soft in** towards the RR. If there are missing withdraws, the only way to get rid of the stale routes is to do a hard clear towards the RR.

  Further Problem Description: The issue was reproduced with the following configuration scale and triggers:

  – DUT(VPNv4 RR) has ~1.2M prefixes.

  - DUT is also connected to other RRs.
  - 4 update-groups and 300 peers.
  - Flap about 30 peers on DUT when there is a churn of 50 prefixes/sec. The churn is stopped after about 15-20sec.
  - Instead of churn, we can also advertise/withdraw 5K prefixes as a trigger.

  This could result in missing updates and withdraws.

- CSCte89956

  Symptoms: Due to PBHK service cannot be synced on standby RP, the session with multiple services including PBHK service is poisoned on standby RP. Then other PPPoE sessions fail to install those ISG services (not including PBHK service) too, while they can successfully be installed on active RP.

  Conditions: This symptom occurs with an ISG service that cannot be synced to standby.

  Workaround: Clear the session on active RP and restart the session.

- CSCtf00132

  Symptoms: A Cisco 7200 series router crashes when there are unauthenticated sessions in a multichassis SGBP environment.

  Conditions: The symptom is observed when multiple unauthenticated sessions in a multichassis multilink PPP SGBP environment are dialed from the same client on multiple home gateways as part of the same session.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(31)SB17

Cisco IOS Release 12.2(31)SB17 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)SB17 but may be open in previous Cisco IOS releases.

- CSCso03047

  Symptoms: The multilink interfaces stop forwarding traffic, and the serial interfaces out of the multilink start to flap.

  Conditions: This symptom is observed when the E3 controller is saturated.

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

- CSCsx13678

  Symptoms: After applying a Run Version, one of the processes is struggling to free up the memory. A traceback is shown with the following error message:

  ```
  00:05:56: %SYS-2-FREEBAD: Attempted to free memory at 6FFFFA9C, not part of buffer
  pool -Traceback= 60680714 6068344C 607DB31C 607DC5BC 607DC668 6065F590 6065F57C
  pre2cm1-5>en
  ```

  Conditions: This symptom occurs when running Cisco IOS Release 12.2(31)SB14.

  Workaround: There is no workaround.

- CSCsy70524

  Symptoms: A router crashes upon deleting range PVCs with PPPoE sessions and with bandwidth configured through DBS.

Conditions: The symptom is observed when deleting the range PVCs with PPPoE sessions.

Workaround: There is no workaround.

- CSCsy81362

  Symptoms: Port-channel VLAN sub-interfaces stop forwarding traffic after an SSO.

  Conditions: The symptom is observed after an SSO. One of the member links is getting removed from the port-channel bundle.

  Workaround: Perform a shut/no-shut the interface.

- CSCsy88764

  SymptomS: ISG PPPoE sessions may lose their authenticated state if they receive Change of Authorization (CoA) for service swapping.

  Conditions: After sending CoA pushes to deactivate an existing service and active new one to ISG PPPOE sessions, the sessions may change state from authenticated to connect. It means the sessions are already in logoff state. As a result, all Subscriber Service Switch (SSS) showings are empty.

  Workaround: There is no workaround.

- CSCsz18711

  Symptoms: NAS-port-ID format reported by AAA accounting VS reply to a CoA account-query are different. Affects back-end server for billing functions.

  Format sent by AAA accounting records:

  ```
  RADIUS: NAS-Port-Id [87] 25 "GigabitEthernet0/1.118:"
  Format sent in reply to CoA Query:
  RADIUS: NAS-Port-Id [87] 33 "nas-port:10.10.10.101:4/0/0/118"
  ```

  Conditions: This behavior was observed in Cisco IOS Release 12.2(33)SB3.

  Workaround: There is no workaround.

- CSCsz20539

  Symptoms: When changing fragmentation from enabled to disabled or vice versa on PRE4, the fragmentation/interleave takes effect dynamically for the non-PQ traffic, but the encapsulation for the PQ traffic did not get changed until the shut/no shut on the interface.

  Conditions: This symptom occurs when enabling or disabling fragmentation on PRE4.

  Workaround: Do a shut/no shut on MLP interfrace after the configuration changes.

- CSCsz62974

  Symptoms: Router crashes while querying for cvpdnTemplateActiveSessions.

  Conditions: Occurs if the vpdn-template name is long.

  Workaround: There is no workaround.

- CSCsz72138

  Symptoms: A POS interface on a PA-POS-2OC3 may experience a stuck issue. All packets will be dropped after hitting the stuck scenario:

  ```
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops:
  72048413<<<<<<<<<<<<<<<<<<<<all packets are getting dropped
    Queueing strategy: Class-based queueing
    Output queue: 197/1000/0 (size/max total/drops)<<<<<<<<<<output queue
  remains stuck at 197
  ```

Conditions: This issue is common to different platforms such as the Cisco 7300, Cisco 7304, and Cisco 7200. Stuck can happen with and without service policy also.

Workaround:

1. Do a “shut”/”no shut” of affected interface.
2. Do a soft OIR of affected slot.

- CSCsz96323

  Symptoms: A Cisco 7301 router crashes with “protocol pptp” configured.

  Conditions: The symptom is observed with a Cisco 7301 router when “protocol pptp” is configured.

  Workaround: There is no workaround.

- CSCta34812

  Symptoms: The offered rate and bandwidth allocated for all the user classes are the same, although different percentages are configured. The output rate failed to guarantee its minimum bandwidth setting.

  Conditions: The data rate for QoS bandwidth is not meeting its minimum requirement.

  Workaround: There is no workaround.

- CSCta36860

  Symptoms: The ISG will have dangling sessions if multiple CoA messages come in while the ISG is making a CoA request.

  Conditions: This symptom occurs when ISG makes a CoA request but never receives a response. During that time, another CoA message comes in to disconnect the session. The session will never be disconnected.

  Workaround: Clear the sessions manually.

- CSCta72272

  Symptoms: A router may crash while doing an OIR of a PA-MC-E3.

  Conditions: The symptom is observed with a Cisco 7200 series router that is running the 122-31.4.57.SB16 image, with frame-relay configurations and with the controller shut.

  Workaround: There is no workaround.

- CSCta73054

  Symptoms: When using passive FTP with NAT VRF, the connection is broken after NAT in the Cisco 7300. The port numbers are not consistent.

  The source port is translated from “X_PORT” to “Y_PORT”, but after NAT to the outside, the port still remains the same. This breaks the passive FTP session.

  Conditions: This issue is observed when using Cisco IOS Releases 12.2(31)SB11, 12.2(31)SB14, 12.2(33)SB3a and 12.2(33)SB5 when using VRF NAT and trying to establish passive FTP connections across the Cisco 7300.

  Workaround: No issues are observed when Cisco IOS Release 12.2(25)S11 is used. The passive FTP session and NAT behave as expected.

- CSCta89550

  Symptoms: On a Cisco 10000 series router with LI done with session brought up via radius and using SNMP session ID taps, LI is not working.

  Conditions: This happens only for using session ID taps in SNMP and bringing up sessions via radius.

Workaround: There is no workaround.

- CSCta91556

  Symptoms: Packets are getting SSS switched on the LAC towards LNS.

  Conditions: The symptom is observed when bringing up any PPPoE or PPPoA session.

  Workaround: There is no workaround.

- CSCta99127

  Symptoms: Spurious memory access is seen on a Cisco router.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 12.2(31)SB14.

  Workaround: There is no workaround.

- CSCtb13546

  Symptoms: A Cisco IOS router crashes with a bus error.

  Conditions: This symptom occurs when a Cisco IOS router is performing multihop VPDN (a.k.a. tunnel switching). The router may infrequently crash due to a bus error.

  This crash is limited to cases where at least one of the following VPDN group commands are configured:

  ip pmtu ip tos reflect

  Workaround: Disable the above mentioned commands. However the consequences of this on user traffic must be evaluated first.

- CSCtb21155

  Symptoms: There is too much traffic in net-control queue. If output interface is an ATM VBR VC, all VCs on the interface may become blocked.

  Conditions: This symptom is observed on Cisco 10000 series routers that are running Cisco IOS Release 12.2SB and acting as MPLS VPN PE routers.

  Workaround: There is no workaround.

- CSCtb52131

  Symptoms: After a core MPLS enabled interface flaps, hardware MAC rewrite resources may leak. If this condition is repeated many times, the MAC resources may become exhausted, and the following log message will be seen:

  ```
  %GENERAL-3-EREVENT: HWCEF: Failed to allocate HW mac rewrite
  ```

  When the resources become exhausted, packet forwarding may be affected. To see if the problem is happening, monitor the following command output:

  ```
  show pxf cpu cef memory
  FP CEF/MFIB/TFIB XCM Type usage:
   Type Name Col Total   Alloc   Size   Start    End      BitMap  Error


    6  Mac  5   524279  77      8      50800000 50C00000 21236D6C 0
  ```

  While the number of routes remains consistent, the Alloc column will increase until it reaches 524279.

  Conditions: After a core MPLS enabled interface flaps, hardware MAC rewrite resources may leak.

  Workaround: The problem can be cleared by performing a router reload, or PRE failover. This will restore all of the MAC rewrites.

- CSCtc05512

  Symptoms: After doing **write erase**, if the router is reloaded, the router may crash or hang.

  Conditions: This issue is seen in Cisco 7200 and Cisco 7300 (NSE100) but is platform independent.

  Workaround: There is no workaround. Avoid the **reload** command after doing **write erase**.

- CSCtc49129

  Symptoms: NAT entries are not timed out after the TCP connection closure. It exceeds the PXF NAT TABLE LIMIT.

  Conditions: This symptom occurs with one NAT entry with one TCP session.

  Workaround: There is no workaround.

- CSCtc51554

  Symptoms: Router crashes when CEF is enabled on an LC interface.

  Conditions:

  - Packet should come from Line Card (SPA, GM, LC).
  - Interface should be Ethernet (FE/GigE).
  - Packet should be TCP/IP encapsulated with dot1Q.
  - NAT translation should happen.
  - Packet is processed in PXF.

  Workaround: Disable CEF on the affected interface or use native interface.

  Further Problem Description: To provide some additional information, this issue was observed following a code upgrade, and the router was in a continuous crash and reload loop due to CEF being enabled globally on the router. With CEF disabled on the affected interface this issue stopped. Once CEF was re-enabled for that interface, the router crashed.

  If an adjacent HSRP neighbor is running the affected Cisco IOS and has CEF enabled, this router will also likely crash once it becomes the active router for the group.

- CSCtc69921

  Symptoms: Memory corruption crash is seen on standby console while unconfiguring the ATM multipoint interface configurations.

  Conditions: A standby PRE crashes due to memory corruption while unconfiguring the ATM multipoint interface configurations when CBR configured pvc-in-range is inactive.

  The crash is not seen when CBR configured pvc-in-range is active.

  Workaround: There is no workaround.

- CSCtc74804

  Symptoms: Two ARP entries for the same MAC are seen on the intelligent service gateway (ISG) acting as a relay.

  Conditions: This symptom occurs when there are multiple DHCP servers there in the deployment, and a delayed offer comes from one of the DHCP servers to DHCP relay (ISG).

  Workaround: Use only a single DHCP server.

Resolved Caveats—Cisco IOS Release 12.2(31)SB16

Cisco IOS Release 12.2(31)SB16 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)SB16 but may be open in previous Cisco IOS releases.

- CSCeh75136

  Symptoms: If a user fails to successfully establish a SSH connection on the first attempt, subsequent attempts may also fail.

  Conditions: Occurs when a Cisco router is configured to authenticate SSH connections using TACACS+. The rem_addr field in the TACACS+ header may be empty if the user does not successfully authenticate on the first attempt. This may cause authentication or authorization failures if rem_addr information is required by the TACACS+ server.

  Workaround: Configure **ipssh authentication-retries 0**.

- CSCek60118

  Symptoms: A traceback may be generated when you configure the L2VPN Pseudowire Redundancy feature.

  Conditions: This symptom is observed on a Cisco 7600 series but may be platform-independent.

  Workaround: There is no workaround. However, note that the functionality of the router is not impacted by the traceback.

- CSCek76288

  Symptoms: With MLPoATM configured, a router crashes when using the **show ppp multilink** command after disabling the PA by the **hw-module slot** *slot- number* **stop** command.

  Conditions: This symptom has been observed on a Cisco 7200 NPE-G1 loaded with Cisco IOS interim Release 12.4(13.13)T2.

  Workaround: There is no workaround.

- CSCsb54378

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

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

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

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

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

```
%SYS-3-CPUHOG: Task is running for (128004)msecs, more than (2000)msecs
(1426/5),process = Virtual Exec.

-Traceback= 0x41DC8E2C 0x41DC9098 0x41BAA6E0 0x41BA6990 0x41B96B4C 0x41BA6768
0x41BA7490 0x41BA7750 0x41BAC854 0x41BA120C 0x40C27024 0x40C26760 0x41BA203C
0x40C73E58 0x40C926E8 0x41834200 %SYS-2-WATCHDOG: Process aborted on watchdog
timeout, process = Virtual Exec.

-Traceback= 0x41A23CC8 0x41BAA3D8 0x41BA6A08 0x41B96B4C 0x41BA6768 0x41BA7490
0x41BA7750 0x41BAC854 0x41BA120C 0x40C27024 0x40C26760 0x41BA203C 0x40C73E58
0x40C926E8 0x41834200 0x418341E4

%Software-forced reload
```

- 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.

- CSCsg00102

  Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

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

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

- CSCsg08751

  Symptoms: Route Switch Processor (RSP) may crash when flash card is removed from RSP slot.

  Conditions: This has been seen on RSP running Cisco IOS Release 12.4(10).

  Workaround: There is no workaround.

- CSCsg33571

  Symptoms: The prefix option is not available under “distribute-list” when configuring “router ospf xxx vrf yyy” (where “xxx” is the OSPF process and “yyy” is the VRF name).

  Conditions: The symptom is observed when running Cisco IOS software.

  Workaround: Use another distribute-list option in place of prefix.

- CSCsi62559

  Symptoms: OSPF packets with IP Precedence 0 are classified by SPD as priority packets. This is an error because only IP Precedence 6 packets should be classified as priority packets by SPD.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2(18) or a later release but may also affect other releases.

  Workaround: Use ACLs to block invalid IP control packets from reaching the control plane.

- CSCsj75448

  Symptoms: On a PRE-2, the output policy attached to the multilink interface gets suspended when the command **microcode reload pxf** is used.

  Conditions: The symptom is observed with the **microcode reload pxf** command.

  Workaround: There is no workaround.

- CSCsk05653

  Symptoms: The **aaa group server radius** subcommand **ip radius source-interface** will cause the standby to fail to sync.

```
c10k-6(config)#aaa group server radius RSIM
 c10k-6(config-sg-radius)#ip radius source-interface GigabitEthernet6/0/0


c10k-6#hw-module standby-cpu reset
 c10k-6#
```

```
%REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_NOT_PRESENT)
%C10K_ALARM-6-INFO: ASSERT MAJOR RP A Secondary
removed
%REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_DOWN)
%REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_REDUNDANCY_STATE_CHANGE)
%REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_NOT_PRESENT)
%REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_DOWN)
%REDUNDANCY-3-IPC: cannot open standby port no such
port
%RED-5-REDCHANGE: PRE B now Non-participant(0x1C11 =>
0x1421)
%REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a
standby insertion (raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

%RED-5-REDCHANGE: PRE B now Standby(0x1421 => 0x1411)
%C10K_ALARM-6-INFO: CLEAR MAJOR RP A Secondary
removed
-Traceback= 415C75D8 4019FB1C 40694770 4069475C
CONFIG SYNC: Images are same and incompatible

%ISSU-3-INCOMPATIBLE_PEER_UID: Image running on peer
uid (2) is the same
 -Traceback= 415CCC2C 415C75FC 4019FB1C 40694770 4069475C
Config Sync: Bulk-sync failure due to Servicing
Incompatibility. Please check full list of mismatched commands via:
   show issu config-sync failures mcl

Config Sync: Starting lines from MCL file:
 aaa group server radius RSIM
  ! <submode> "sg-radius"
 - ip radius source-interface GigabitEthernet6/0/0
```

Conditions: This symptom is observed if the **aaa group server radius** subcommand **ip radius source-interface** CLI is configured on a box with dual PREs.

Workaround: If the customer does not use the **aaa group server radius** subcommand **ip radius source-interface** *interface*, this will not be a problem.

If they use the **aaa group server radius** subcommand **ip radius source-interface** *interface* on a Cisco 10000 router in simplex mode (a single PRE), this will not be a problem.

If they run with dual PREs, then they will need to remove the **aaa group server radius** subcommand **ip radius source- interface** *interface* from the configuration as a workaround.

Removing the **aaa group server radius** subcommand **ip radius source-interface** *interface* from the configuration could cause problems for the customer. The radius server may be expecting the request to come from a specific source address. The router will now use the address of the interface the packet egresses the router from, which may change over time as routes fluctuate.

- CSCsk21328

  Symptoms: Router crashes during shutdown or deletion of interface.

  Conditions: Occurs on interfaces on which IPv6 is enabled.

  Workaround: There is no workaround.

- CSCsk23972

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

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

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

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

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

- CSCsk58716

  Symptoms: The following error message is seen:

  ```
  GENERAL-3-EREVENT: HWCEF: Failed to allocate HW mac rewrite
  ```

  Conditions: The symptom is observed with a Cisco 10000 series router under rare conditions during a route flap.

  Workaround: Reload the PRE.

- CSCsk83505

  Symptoms: Under various circumstances, UDP input queues can grow to much larger than their intended size. This can result in memory allocation errors if the application that services a UDP input queue is unable to do so quick enough to keep up with incoming traffic. UDP needs to drop received packets, once a given input queue has reached its limit.

  Conditions: This symptom is observed with RIPv6 with a large number of neighbors in both Cisco IOS and ION images.

  Workaround: There is no workaround.

  Further Problem Description: The root cause is that several pieces of code are enqueuing packets to ipsocktype inQ without checking its size, and without updating statistics.

- CSCsk96581

  Symptoms: After loading a router for the first time or performing a switchover with a large number of BGP neighbors configured, some neighbors may send hold timer expired notifications before reaching established state.

  Conditions: The problem is seen on routers with highly scaled configurations with many BGP neighbors with low hold timers configured. Typically, the problem is most likely to be seen after a switchover happens when all interfaces on the new active RP come up at approximately the same

time. The sudden burst of sessions attempting to establish at the same time can cause some of the sessions to fail to be serviced in time to satisfy aggressive hold timers. Established sessions are not vulnerable to this issue; only sessions in progress to established state can experience the problem.

Workaround: BGP neighbors can be brought up in smaller groups rather than all at once to distribute the session establishment load so that no session in progress to established state will exceed their configured hold timers.

- CSCsl39986

  Symptoms: The changes introduced by Cisco bug ID CSCsi73899 introduced some performance impact.

  Conditions: Only Cisco IOS versions with CSCsi73899 integrated and not CSCsl39986 are affected. These images are only interim images and should not be available on Cisco.com for general download purposes.

  Workaround: There is no workaround.

- CSCsl62076

  Symptoms: Configuring IPv6 RIP on a router may cause the router to crash.

  Conditions: The symptom is observed on a Cisco 10000 series router when configuring IPv6 RIP.

  Workaround: There is no workaround.

- CSCsm64307

  Symptoms: When PPP sessions are terminated, the standby NPE may crash. This is true for both PPP sessions that are terminated naturally (from the customer end), and those that are terminated prematurely (at the provider end due to a command such as **clear pppoe sessions all**).

  Conditions: At present the conditions are unknown. It only appears to impact 12.2(31)SB10 and related releases.

  Workaround: There is no workaround.

- CSCsm70668

  Symptoms: A soft OIR over E3:POS impacts complete traffic with a biscuit tunnel.

  Condition: A soft OIR over E3:POS impacts complete traffic with a biscuit tunnel configured. In OIR “test mbus power 6 off” and “test mbus power 6 on” are performed followed by a microcode reload on slot 6.

  Workaround: There is no workaround.

- CSCso50347

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

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

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

- CSCso71955

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

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

  Workaround: Disable netflow if possible.

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

- CSCsq09962

  Symptoms: Cisco 7600 router crashes at “pim_proxy_empty_rd.”

  Conditions: Customer seeing crash with decode during initial deployment of new Cisco 7600 router.

  Workaround: There is no workaround.

- CSCsq77043

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

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

  Workaround: Reduce the size of the hostname.

- CSCsq80589

  Symptoms: During a maintenance window, a Cisco 7206VXR router is upgraded from an NPE-G1 to an NPE-G2. The router comes up normally after the swap, but about 10 minutes later the router crashes. When it comes up again, the configuration is checked, but the router crashes again.

  The following error message is seen:

  ```
  "Unexpected reboot due to SegV Exception" (as indicated by show version)
  ```

  Conditions: This symptom is observed when upgrading a Cisco 7206VXR from an NPE-G1 to an NPE-G2.

  Workaround: There is no workaround.

- CSCsq86500

  Symptoms: The following error message is displayed when the standby is reloaded:

  ```
  "REDUNDANCY-3-IPC: cannot open standby port no such port"
  ```

  Conditions: No specific condition.

  Workaround: There is no workaround. The error message is harmless and does not affect the functionality of the router in any way.

- CSCsr17660

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

  Conditions: Occurs when BGP and VPNv4 are configured.

  Workaround: There is no workaround.

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

- CSCsr51801

  Symptoms: Some of the route-maps configured for BGP sessions (eBGP) are not permitting the prefixes upon a router reload.

  Conditions: The symptom is observed when a large number of route-maps for a BGP session are configured and the router is reloaded.

  Workaround: Issue the command **clear ip bgp * soft**.

- CSCsr53059

  Symptoms: A PPPoA session fails to come up after modifying the PVC.

  Conditions: The symptom was seen while testing the feature PPP over ATM with Subscriber Service Switch.

  Workaround: There is no workaround.

- CSCsr96042

  Symptoms: ASR1000 Router crashes.

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

  Workaround: There is no workaround.

- CSCsr97753

  Symptoms: Pinging an interface fails.

  Conditions: Occurs when unconfiguring xconnect on the interface.

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

- CSCsu27888

  Symptoms: IGMP v3 reports are discarded.

  Conditions: Occurs on Cisco 7200 router running Cisco IOS Release 12.4(20)T2.

  Workaround: There is no workaround.

- CSCsu37317

  Symptoms: A Cisco 7500 router crashes.

  Conditions: IMA interface is configured with three and four members each. Attach service policy to an IMA pt interface. Now try to remove the IMA pt interface.

  Workaround: There is no workaround.

- CSCsu61813

  Symptoms: Line cards may reset during ISSU upgrade even when there is no change in the major number.

  Conditions: This symptom may occur during ISSU upgrade even though there is no change with the major number of line card images.

  Workaround: There is no workaround. However the line card comes up fine after the reset.

- CSCsv16421

  Symptoms: The cbQosCMDropPkt64 object does not work on the PE-CE policy with priority police command. The value stays at 0.

  Conditions: The symptom is observed when Priority is configured with policy. The cbQosCMDropPkt count stays at 0 during snmpwalk.

  Workaround: There is no workaround.

- CSCsv27607

  Symptoms: BGP router filters outbound routes to the peers when doing soft reset with specifying peer address using the **clear ip bgp** *ip-addr* **soft out** command. However, the routes to be filtered are not deleted from the routing table on the BGP peer router.

Conditions: The symptom happens when removing and then reapplying an outbound route-map. When issuing the **clear ip bgp** *neighbor-address* **soft out** command for each peer in an update-group after applying the outbound route-map filtering policy. The withdraw for filtered prefixes is sent to the first peer specified in soft reset, but the next peers in the same update-group do not withdraw the routes.

Workaround: Perform a hard BGP reset using the **clear ip bgp** *ip-addr* command.

- CSCsv31342

  Symptoms: QoS does not work when a very large number of class-maps and ACLs are configured.

  Conditions: The symptom is observed on an NSE-100/NSE-150 when a large number of class-maps and ACLs are configured, so that the maximum policy-maps supported by the result table become less than 2048 (this can be checked using the **test platform acl** command). QoS does not work due to the QoS lookup table not getting updated correctly.

  Workaround: Removing and reconfiguring all the service-policies is the only workaround.

- CSCsv34532

  Symptoms: The packet length field incorrectly indicates the length is “zero”.

  Conditions: During any use of PPPoE, the length is not available. Thus the law enforcement device that catches the stream is not able to calculate correctly.

  Workaround: There is no workaround.

- CSCsv73754

  Symptoms: A Cisco 10000 series router crashes. Traceback decode points to a function of bgp_vpn_impq_add_vrfs_cfg_changes.

  Conditions: The symptom is observed while unconfiguring VRFs. It is most likely to be seen when 100 VRFs or more are unconfigured.

  Workaround: There is no workaround.

- CSCsv76018

  Symptoms: A NSE-100 crashes after an SSO when traffic is kept on for one AToM-PPPoE circuit.

  Conditions: The symptom occurs after an SSO with traffic running for AToM-PPPoE.

  Workaround: There is no workaround.

- CSCsv91602

  Symptoms: Cisco 7201 with Gi0/3 experienced communication failure.

  Conditions: This problem does not occur with Gi0/0 or Gi0/2.

  Workaround: Perform a **shut/no shut** on the Gi0/3. The problem will occur again.

- CSCsw16133

  Symptoms: SWIDBs are not cleared, even after removing the subinterfaces. Deleted subinterfaces are considered to be inactive VCs which block the configuration of the maximum number of IDs on the interface.

  Conditions: The symptom is observed when subinterfaces are created using the **range pvc** command. If the subinterfaces are deleted, this is not updated in the SWIDBs.

  Workaround: Reload the router.

- CSCsw19729

  Symptoms: Basic ping on the serial interface does not work after a reboot.

Conditions: The symptoms occur with any encapsulation with an NSE-100 and NSE-150.

Workaround: Explicitly do the encapsulation configuration. Even configuring the same interface will work.

- CSCsw24542

  Symptoms: A router may crash due to a bus error after displaying the following error messages:

  ```
  %DATACORRUPTION-1-DATAINCONSISTENCY: copy error,
  %ALIGN-1-FATAL: Illegal access to a low address < isdn function decoded>
  ```

  Conditions: The symptom is observed on a Cisco 3825 router that is running Cisco IOS Release 12.4(22)T with ISDN connections.

  Workaround: There is no workaround.

  Further Problem Description: When copying the ISDN incoming call number for an incoming call from Layer2, the length of the call number was somehow exceeding the maximum allocated buffer size (80). PBX has pumped a Layer2 information frame with call number exceeding the maximum number length limit. It leads to memory corruption and a crash.

- CSCsw27711

  Symptoms: GE SPA does not come up after performing multiple times **shut** and **no shut**. The following error message is shown:

  ```
  %SPA_ETHER-3-SEND_MSG: Subslot 4/0, 2xGE SPA Failed to notify driver process about a
  line state change in one of the SPA interfaces
  ```

  Conditions: The symptom occurs after performing multiple times **shut** and **no shut** and having around 1000 SPA-GIG subinterfaces.

  Workaround: Perform **hw-module slot** *slot-number* **stop/start** to bring up the interface.

- CSCsw47210

  Symptoms: Range PVCs fail to come up on the interface when a VC-class with create-on-demand is detached from the ATM interface.

  Conditions: The symptoms are observed when a VC-class with create-on-demand is detached from the interface.

  Workaround: Remove create-on-demand from the VC-class instead of removing the VC-class itself.

- CSCsw62823

  Symptoms: Encapsulation is not getting inherited from the VC-class for the final VC.

  Conditions: The symptom is observed when changing encapsulation from the console without exiting from the applied encapsulation under VC-mode on a VTY session.

  Workaround: Apply encapsulation from single terminal at the same time (either from console or from VTY).

  Further Problem Description: Only the last VC is not getting updated with encapsulation.

- CSCsw65933

  Symptoms: The CE does not learn the prefix from one of the PEs.

  Conditions: The symptom is observed after configuring (on PE2):

  ```
  router bgp 10
    address-family ipv4 vrf test1
    no neighbor <peer > route-map setsoo in
    end
  ```

and then clearing using the following command: **clear ip bgp** *peer vrf test1* **soft out**.

Workaround: Use the command **clear ip bgp * soft** on the PE after SOO is applied.

Alternate Workaround: On the CE, the command **clear ip bgp * soft** should not be applied within one minute after applying SOO route map to CE on UUT.

- CSCsw72030

  Symptoms: A NSE-100/150 crashes when you configure and bring up an L2TP xconnect circuit over a GRE tunnel.

  Conditions: The symptom occurs when you configure an L2TP circuit over a GRE tunnel and bring up the circuit by making the xconnect interface up.

  Workaround: There is no workaround. You can disable PXF via the configuration command **no ip pxf** to avoid this problem. The downside being all traffic will be RP-switched at a much slower rate than PXF-switching.

- CSCsw76692

  Symptoms: PXF crashes when traffic is sent for an L2TPv3 circuit which has been configured over a GRE tunnel.

  Conditions: The symptom occurs when the core-facing interface is ATM and the peer router is a non-PXF.

  Workaround: There is no workaround.

- CSCsw87061

  Symptoms: A Cisco 7304-NSE100 router crashes when configured with NAT and a large number of ACLs.

  Conditions: This symptom occurs when configuring NAT with a large number of ACLs. A malloc failure will occur and will be followed by the router crash. This happens only on NSE100 and not on NSE150.

  Workaround: There is no workaround.

- CSCsw91422

  Symptoms: Crash occurs on Cisco 7206VXR/NPE-G1 running Cisco IOS Release 12.2(31)SB12.

  Conditions: Occurs under general use. No error messages appear in logs.

  Workaround: There is no workaround.

- CSCsx06457

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

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

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

- CSCsx13929

  Symptoms: The following error is observed when you flap the Native gig interface through which an L2TP circuit over a GRE tunnel is configured and when traffic is passing:

  ```
  %NSE100-3-VA_ERROR: Vanallen ASIC detected an error condition: SROC packet length
  missmatch
  ```

Conditions: The symptom occurs when PFX is enabled and traffic is passing through the circuit.

Workaround: There is no workaround.

- CSCsx23000

  Symptoms: Configurations on an ATM card are not removed. Tracebacks and error messages are displayed, and the router may crash.

  Conditions: This symptom is observed when you have range-pvc configured under p2p atm subifs, irrespective of the card type. With scaling configurations like 8k range VCs on each port of 4oc3atm card, the router may crash.

  ```
  hw-module slot<> shut
    no card <>
  ```

  Workaround:

  - Reload the box when the problem occurs.
  - To avoid the problem from happening, if you have p2p interface with range- pvc configurations, remove all those configurations using the **no interface** command before doing “no card”.

- CSCsx23419

  Symptoms: The SFP ports are shown in the ENTITY MIB even though the SFPs are not inserted.

  Conditions: The symptom is observed with an NPE-G2 and NSE-150 card running Cisco IOS Release 12.2(31)SB10.

  Workaround: There is no workaround.

  Further Problem Description: In both (shut/no shut) states the issue occurs. With the ANA model, the device operates correctly the first time when the SFP is inserted (SFPmodule ==> SFP container ==> port). But once the SFP is pulled out, the port goes under the container (incorrectly, as the port should not go there). When we insert the SFP, the same port comes under the module. Since ANA will not delete a DC (the port, in this case) the same port gets two parents which ANA will not accept. With this fix the "PORT" entry will not be populated by the ENTITY MIB unless XCVR exists.

- CSCsx28221

  Symptoms: A router crashes.

  Conditions: The symptoms are seen when configuring range PVCs on a point-to-point subinterface and creating PPPoA sessions.

  Workaround: There is no workaround.

- CSCsx28442

  Symptoms: Spurious memory access may be observed with a Cisco 7304 (NPEG100) router when PA-CC is booting up with any channelized PAs, such as PA-MC-T3/PA-MC-E3/PA-MC-8TE1/PA-2CT3+/and other channelized PAs.

  Conditions: The symptom is observed when booting up a Cisco 7304 (NPEG100) RP which has PA-CC with channelized PA, or when the PA-CC with channelized PA is inserted. It is seen with the latest Cisco IOS 12.2(33)SB images (after release 12.2(33)SB3).

  Workaround: There is no workaround.

- CSCsx28948

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

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

Workaround: There is no workaround.

- CSCsx29123

  Symptoms: An E1 flaps due to LOF/RAI alarms.

  Conditions: The symptom is observed after an upgrade to Cisco IOS Release 12.0(30)SZ from Release 12.0(28)S5.

  Workaround: Toggle the E1 clock source from line to internal or internal to line.

  Alternate Workaround: Apply a local loopback then remove the loopback.

- CSCsx31786

  Symptoms: A Cisco 10000 series router that is running Cisco IOS Release 12.2(31)ZV2a may reboot or lose communication with all line cards (displaying an “IPCOIR-3-TIMEOUT” message).

  Conditions: The symptom is observed after a PPPoE session establishment and when IGMP joins to one multicast stream with many receivers.

  Workaround: There is no workaround.

- CSCsx34297

  Symptoms: Watchdog reset seen with combination of NPEG1+PA-POS-1OC3/PA-POS-2OC3.

  Conditions: The symptom is observed on a Cisco 7200 series router and Cisco 7301 router with an NPEG1 processor.

  Workaround: Change the MDL of operation to PULL using the command **dma enable pull model**.

- CSCsx43644

  Symptoms: Policy-name remains unchanged after renaming.

  Conditions: The symptom is observed only with an ATM interface.

  Workaround: There is no workaround.

- CSCsx49444

  Symptoms: PVCs associated with an F4 OAM VP remain in an “INAC” state after the interface flaps.

  Conditions: The symptom is observed with F4 OAM management configured on a VP.

  Workaround: Use the commands **shut** followed by **no shut** again.

- CSCsx64198

  Symptoms: Intercepted LI packets are not updated in MIB counter.

  Conditions: This symptom is observed when creating time based ACL for taps.

  Workaround: There is no workaround.

  Further Problem Description: Intercepted packet count is based on packets sent to MD. For time based ACL, it is not getting incremented although MD is receiving the packets. Due to this time based ACL script for LI, count fails.

- CSCsx70889

  Cisco devices running affected versions of Cisco IOS Software are vulnerable to a denial of service (DoS) attack if configured for IP tunnels and Cisco Express Forwarding.

Cisco has released free software updates that address this vulnerability.

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

- CSCsx78529

  Symptoms: A Cisco router may crash when a policy map is simultaneously displayed and unconfigured.

  Conditions: The symptom occurs when the **show policy-map** command is entered via one CLI session while the **no policy-map** *policy-map-name* command is entered via another CLI session.

  Workaround: Avoid making complicated modifications to the policy map when it is being shown in another session.

- CSCsy07789

  Symptoms: QoS classification is broken with two user-defined classes.

  Conditions: The symptom is observed on a Cisco 7300 (NSE-100) and 7300 (NSE-150) router.

  Workaround: There is no workaround.

- CSCsy14633

  Symptoms: Packets are not getting intercepted.

  Conditions: The symptoms are observed when using radius-based LI.

  Workaround: There is no workaround.

- CSCsy15227

  Cisco IOS Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

  There are no workarounds that mitigate this vulnerability.

  This advisory is posted at the following link:

  http://www.cisco.com/warp/public/707/cisco-sa-20090923-auth-proxy.shtml

- CSCsy21284

  Symptoms: Half-Duplex VRF (HDVRF) does not forward packets on a downstream VRF.

  Conditions: The symptoms are observed when running HDVRF on LNS with the upstream/downstream VRFs passing over a LACP port-bundle. The packets are passed upstream towards the destination, however, the return packets are dropped before they are passed to the PPP client.

  Workaround: There is no workaround.

- CSCsy22215

  Symptoms: Multicast traffic drops in MVPN setup. Mroute entry in ingress PE stays in “Registering” state.

  Conditions: The symptom is observed in an MVPN setup.

  Workaround: Configuring “ip pim fast-register-stop” in the router that is configured as RP will fix the problem in most cases.

- CSCsy26830

  Symptoms: The network address of the former network is not reachable after a subnet change, if “unicast RPF” is configured on the interface.

Conditions: The symptom is observed when running Cisco IOS Release 12.2(31)SB13 and 12.2(31)SB14 and when “unicast RPF” is configured.

Workaround: Reload the router or remove “ip verify unicast source reachable-via any” from the interface.

- CSCsy32368

  Symptoms: An 8192 hold-queue value for the port-channel is invalid.

  Conditions: The symptom is observed when two interfaces, each with a hold-queue of 4096, are configured and then added to the port-channel interface. The hold-queue value of the port-channel is 8192 which is invalid.

  Workaround: There is no workaround.

- CSCsy39667

  Symptoms: On a PPP aggregator using dhcp-proxy-client functionality, in a situation where a PPP client session is torn down and then renegotiated within 5 seconds, the DHCP proxy client may send a DHCP RELEASE for the previous DHCP handle after the new DHCP handle (created as a result of new IPCP CONFREQ Address 0.0.0.0) has accepted the same IP address allocation from the offnet DHCP Server. This results in the offnet DHCP server having no record of the lease as it exists on the PPP aggregator which causes future addressing conflicts.

  Conditions: The symptom is observed on a Cisco 7200 (NPE-400) and 7200 (NPE-G2) that is running Cisco IOS Release 12.4 T, or 12.2 SB.

  Workaround:

  1. Automated: Write a script to compare active leases on the PPP aggregator to active leases on DHCP server. If a lease is found to only exist on the PPP aggregator, use **clear interface virtual-access** to recover.
  2. Manual: use the command **clear interface virtual-access**.

  Further Problem Description: This issue occurs because the DHCP client holdtime is static at 5 seconds and there are no IOS hooks to tie PPP LCP session removal and IPAM to suppress stale DHCPRELEASES waiting in queue for HOLDTIME to expire.

- CSCsy49524

  Symptoms: A Cisco 7304 router may crash due to memory corruption.

  Conditions: The symptoms are observed with an Any Transport over MPLS (AToM) tunnel being transported over a Generic Routing Encapsulation (GRE) tunnel. LDP is enabled on the tunnel and routes to the LDP neighbor are known via the tunnel interface. The crash usually occurs during initial bootup when the remote LDP neighbor comes up, but has also been observed after a period of normal operation (specifically seen while transporting ATM over MPLS).

  Workaround: There is no workaround.

- CSCsy54233

  Symptoms: The exception_reserve_memory is invalid in unix image.

  Conditions: Unix images do not support exception_reserve_memory.

  Workaround: There is no workaround.

- CSCsy54440

  Symptoms: A standby, which is running Cisco IOS Release 12.2(31)SB, will crash while upgrading to Cisco IOS Release 12.2(33)SB, after using the command **issu runversion**.

Conditions: The symptom is observed while upgrading from Cisco IOS Release 12.2(31)SB to Cisco IOS Release 12.2(33)SB after using the command **issu runversion** and when there is one or more PPPoE sessions present.

Workaround: Ensure there are no PPPoE sessions present while upgrading.

- CSCsy58115

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

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

  - 12.2(31)SB14
  - 12.2(33)SB1b
  - 12.2(33)SB2
  - 12.2(33.05.14)SRB
  - 12.2(33.02.09)SRC
  - 12.2(33)SRC3
  - 12.4(20)T2
  - 12.4(22)T1
  - 12.2(33)SXI or later releases.

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

- CSCsy59142

  Symptoms: The port in the line card cannot create a PPPoE session. The **show controller atm** *1/0/0* command shows that the counter “non-existent VC” is increasing.

  Conditions: The symptom is observed with a Cisco 10000 series router with ATM PPPoE sessions.

  Workaround: Reconfigure the interface.

  Further Problem Description: For the multiport OC3ATM card, having any physical interface in shut state with non default MTU configured on any of its subinterfaces or the physical interface itself, the following sequence of operations can cause a SAR corruption and traffic failure:

  - hw-module reset of the card or router reload.
  - no-shut the physical interface.

  After the no-shut event, all the VCs under other physical interfaces of the multiport card may drop traffic.

- CSCsy61277

  Symptoms: A router may crash when using the **show cef int** command in parallel with removing per-user ACL via radius.

  Conditions: The symptom is observed when using the **show cef int** command in parallel with removing per-user ACL via radius.

  Workaround: There is no workaround.

- CSCsy75718

  Symptoms: On a PPP aggregator using dhcp-proxy-client functionality, in a situation where a PPP client session is torn down and then renegotiated within 5 seconds, the DHCP proxy client may send a DHCP RELEASE for the previous DHCP handle after the new DHCP handle (created as a result of new IPCP CONFREQ address 0.0.0.0) has accepted the same IP address allocation from the offnet DHCP Server. This results in the offnet DHCP server having no record of the lease as it exists on the PPP aggregator which causes future addressing conflicts.

  Conditions: The issue appears to be Day 1, reported on a Cisco 7200/NPE-400 and 7200/NPE-G2 that is running Cisco IOS Release 12.4T, 12.4M, or 12.2SB.

  Workaround:

  1. Automated: Write a script to compare active leases on the PPP aggregator to active leases on DHCP server and if a lease is found only to exist on PPP aggregator, use the command **clear interface virtual-access** to recover.

  2. Manual: use the command **clear interface virtual-access**.

  Further Problem Description: The issue occurs because the DHCP client holdtime is static at 5 seconds and there are no IOS hooks to tie PPP LCP session removal and IPAM to suppress stale DHCPRELEASES waiting in queue for HOLDTIME to expire when the PPP user's virtual access interface changes.

  Note: Use case fixed via CSCsy39667:

  1A. PPP session with userid "jerry", VAI 100, and va_swidb "X" goes down. 1B. New PPP session with userid "jerry", VAI 100, and va_swidb "Y" is negotiated within 5 seconds of 1A.

  Fix Overview: DHCP looks for match on PPP userid and VAI number (not va_swidb) to reclaim DHCP Lease.

  Use-case still requiring a fix:

  2A. PPP session with userid "jerry" and VAI 100 goes down. 2B. New PPP session with userid "jerry" and VAI 200 is negotiated within 5 seconds of 2A.

- CSCsy82158

  Symptoms: A corrupt multicast packet may crash the PXF on a Cisco 10000 series router with the following exception error:

  ```
  "PXF DMA Error -Small Packet Handle Creating a Large Descriptor, Restarting PXF"
  ```

  Conditions: The issue is seen when a padded multicast packet is switched by the PXF and the IP length, from the IP Header, does not include this padding.

  For example, a multicast packet where the IP length is 124 bytes and there is 436 of unaccounted padding can crash the PXF with a "PXF DMA Error".

  Workaround: There is no workaround.

- CSCsz01313

  Symptoms: A router crashes with the following message:

  ```
  MET-DST: %SYS-2-INTSCHED: 'may_suspend' at level 7
  -Process= "AAA SEND STOP EVENT", ipl= 7, pid= 230
  -Traceback= 406ED098 406CEF8C 409E6A48 409E71F4 409E7CBC 406A1218 40875D20 40875D98
  400E89F0 40180A78 406F2708 406F2A00 406E88A0 406D7AE4 406E7A14 406E3B08
  ```

  Conditions: The symptom is observed under normal operation.

  Workaround: There is no workaround.

- CSCsz01484

  Symptoms: When using CBR-ATM traffic class on a ESR OC12 or OC3 line card for PPPoATM over MLP over MultiVCs, only half of the VAI sessions come up active in the bundle. If VBR-NRT is used, the problem does not occur.

  Conditions: The symptom is observed with Cisco IOS Release 12.2(31)SB or later.

  Workaround: For the ESR-4OC3ATM-SM-LR a possible workaround would be to use VBR-NRT. However, this is not an option for the 1oc12atm-1 card since CBR and VBR-NRT use a different SAR scheduler.

- CSCsz14873

  Symptoms: Auto-RP messages are not forwarded from a Cisco 10000 series router PE to any attached CE in MVPN.

  Conditions: The symptom is seen with an MVPN setup, when Auto-RP routes have both an L and H flag.

  Workaround: There is no workaround.

- CSCsz17966

  Symptoms: A PXF restart is reported the pxf crashinfo as follows:

  ```
  PXF DMA Error - Command Byte Length Equals Zero
  PXF DMA Error - Input Command Has Sequence Problem
  ```

  Conditions: This issue is seen on a Cisco 10000 series router that is running Cisco IOS Release 12.2(31)SB13. It is seen when receiving malformed LFIoATM fragments.

  Workaround: There is no workaround.

- CSCsz21640

  Symptoms: A router may crash with BusError when sending an AccountingStop record.

  Conditions: Just before the crash, the following error messages are seen:

  ```
  %IDMNGR-7-ALLOCFAIL: Warning: Failed to allocate memory for keylist in event_init
  %IDMNGR-7-ALLOCFAIL: Warning: Failed to allocate memory for client request data in
  request_init
  ```

  The system is configured for ISG-services.

  Workaround: There is no workaround.

  Further Problem Description: This was seen in a customer specific special based on Cisco IOS Release 12.2(31)SB13.

- CSCsz30049

  Symptoms: A router may crash with memory corruption or with one of the two following messages:

  ```
  %SYS-6-STACKLOW: Stack for process HQF Shaper Background running low, 0/6000
  %SYS-6-STACKLOW: Stack for process PPP Events running low, 0/12000
  ```

  In the case of memory corruption, a corrupted block will be in an address range very close to process or interrupt level 1 stack (this information is available in the crashinfo file).

  Conditions: The symptom is observed on routers running Cisco IOS Release 12.2SB when ALL of the following conditions are met:

  1. The router is configured for VPDN/L2TP.
  2. There is a mixture of PPPoVPDN and “MLP Bundle” users.
  3. QoS service policy with queuing actions (bandwidth guarantee or shaper) is applied to virtual access interfaces for both types of users.

Here is a way to find out if there is normal PPP users or MLP users:

```
PPP User via CLI:
 Router#sh user | inc PPP.*00 [1-9]
   Vi4          user#wl-cp03-7k2#4 PPPoVPDN     00:00:00 30.3.0.47

 MLP via CLI:
 Router#sh user | inc MLP.*00 [1-9]
   Vi8          user#wl-cp04-7k2#5 MLP Bundle   00:00:00 30.4.0.54
```

Workaround:

1. Allow only PPPoVPDN (i.e.: prevent “MLP Bundle” creation).
2. Disable QoS for “MLP Bundle” users or all users.

- CSCsz42795

  Symptoms: A Cisco 10000 series router crashes immediately after the application of QoS on a recently-created serial subinterface.

  Conditions: The symptom is observed if the ATM subinterface is removed from the configuration and a new serial interface is created.

  Workaround: There is no workaround.

- CSCsz43691

  Symptoms: If TAL subscribers attempt to logon when the Cisco ASR 1000 series router RADIUS service download requests a time-out, some sessions will get stuck in “Attempting” state during user/service authorizations. Once 200 sessions are stuck in this state, no subscriber will be able to login until all the sessions (those that are active and those that are stuck in “Attempting” state) are manually cleared using the **clear subscriber session all** command.

  Conditions: The symptom is observed when TAL subscribers attempt to logon while the Cisco ASR 1000 series router RADIUS service download requests a time-out.

  Workaround: Use the **clear subscriber session all** command to manually clear all sessions. This may be, however, service disruptive and impractical in a production network.

- CSCsz50620

  Symptoms: Bus error crash at an invalid address.

  Conditions: The symptom is observed when running Cisco IOS Release 12.2(31)SB with SSS configured.

  Workaround: There is no workaround.

- CSCsz56805

  Symptoms: Different IPs are seen on the same session between Active and Standby PRE cards and the number of in-use IP addresses on Standby is more than that on the Active.

  Conditions: The symptom is observed with the frequent connect/disconnect of sessions and when IP addresses are allocated from the local pool.

  Workaround: Reload the Standby card frequently.

- CSCsz58120

  Symptoms: IP tapping for TAP fails when only source or destination is specified.

  Conditions: The symptom is observed with the following conditions:

  1. Only source or destination specified in TAP request.

2. There are multiple subnets in the target IP class network.

Workaround: Specify both source and destination.

- CSCsz70515

  Symptoms: A PXF crashes when a fragment with zero payload is received. PXF crashes with signature PXF DMA Error: Command Byte Length Equals Zero.

  Conditions: The symptom is observed when an IP fragment (first or last) with zero payload is received.

  Workaround: There is no workaround.

- CSCsz71654

  Symptoms: Accounting records do not show the correct username.

  Conditions: The symptom is observed when account-logon (authentication) happens after failed Transparent Auto-Logon (TAL).

  Workaround: There is no workaround.

- CSCsz81855

  Symptoms: Link-local IP is not able to be pinged if uRPF is enabled on the interface.

  Conditions: The symptom is observed when an RPF check is enabled on IPv6 interfaces connected back-to-back.

  Workaround: There is no workaround.

- CSCsz84703

  Symptoms: IPv6 global ping fails, if uRPF is enabled in a back-to-back setup.

  Conditions: The symptom is observed when RPF is enabled on back-to-back IPv6 interfaces. If a **shut** and **no shut** is done on one of the interfaces, a ping initiated from the other end fails.

  Workaround: There is no workaround.

- CSCsz97358

  Symptoms: A router crashes due to memory corruption.

  Conditions: The symptom is observed on a Cisco 7300 series router (with an NSE-150) that is running Cisco IOS Release 12.3(31)SB14.

  Workaround: There is no workaround.

- CSCta00720

  Symptoms: Attempting an auto proxy logon causes a crash.

  Conditions: This crash is seen only with auto proxy service download.

  Workaround: If services are activated by CoA service logon, this issue will not be seen.

  Further Problem Description: Attempting authentication of the proxy service causes a crash with traceback in description when the user profile is similar to:

```
simulator radius subscriber 1
 framed protocol ppp
 service framed
 authentication rouble-auto password cisco
 vsa cisco 250 Aproxy_service;proxy_user;welcome
 vsa cisco generic 1 string "accounting-list=default"
!
```

- CSCta06499

  Symptoms: The process memory available in the system decreases over time.

  Conditions: The symptom is observed when there are many failures of the service-policy configuration.

  Workaround: Locate the failed policies and change them so that policy can be applied successfully.

  Further Problem Description: The memory leak comes from HQF chunk memory. Every time a policy fails to attach, there is one chunk leaked.

Resolved Caveats—Cisco IOS Release 12.2(31)SB15

Cisco IOS Release 12.2(31)SB15 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)SB15 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCsj07189

  Symptoms: Entering the **snmpget** of an object identifier (OID) using the interface index (ifIndex) value of an interface for its index will result in an error:

```
snmpget -c <community> -v1 <device> IF-MIB::ifDescr.92
Error in packet
Reason: (noSuchName) There is no such variable name in this MIB.
Failed object: IF-MIB::ifDescr.92
```

  Conditions: This can occur after port adapters (PA) have been swapped, such as replacing a 4-port PA with an 8-port PA.

  Workaround: Use the **snmpwalk** command to retrieve the IF-MIB values.

- CSCsj56281

  Symptoms: Inherit peer-policy does not work after router reload.

  Conditions: This symptom occurs after reloading the router.

  Workaround: There is no workaround.

- CSCsk61411

  Symptoms: A memory leak is observed pointing to alloc pc strcat_with_realloc when using the CLI policy-map type service command and its subcommands.

  Conditions: The following CLIs cause the memory leak:

```
Router(config)#policy-map type service my_service
Router(config-service-policymap)#?
policymap-service commands:
  <0-1000>          priority number
  authenticate      Configure authentication parameters
  class             Specify a class-map to match against for this policy-map
  classname         DHCP policy classname
  default           Set a command to its defaults
  exit              Exit from policy-map service configuration mode
```

```
ip                IP configuration
keepalive         keepalive for IP subscriber session
no                Negate a command or set its defaults
policy-name       Policy name delegated to External Policy Delegation device
pppoe             Configure PPPoE related commands
service           service types
service-monitor   Service Monitoring options for external policy
service-policy    Configure QoS Service Policy
sg-service-group  SG Service Group (VRF) parameters
sg-service-type   SG Service Type parameters
```

Workaround: There is no workaround.

- CSCso54167

  Symptoms: BGP peers are stuck with table versions of 0. BGP peers do not announce any routes to neighbors.

  Conditions: Whenever the interfaces flap with online insertion and removal (OIR) multiple times, all of the BGP peers using such interfaces for peering connections encounter this issue.

  Workaround: Delete and reconfigure the neighbor.

- CSCso90058

  Symptoms: MSFC crashes with RedZone memory corruption.

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

  Workaround: There is no workaround.

- CSCso92930

  Symptoms: Available memory may decrease over time on a Cisco ASR1000 RP as subscribers connect and disconnect.

  Conditions: This symptom is observed when the Cisco ASR1000 functions as a LAC or LNS. AAA accounting is enabled for tunnel, session and PPP.

  Workaround: If the available memory decrease impacts system functions, disable AAA accounting as a temporary remedy.

- CSCsr70963

  Symptoms: A Cisco 10000 PRE will reload unexpectedly when a radius server which is marked as dead is removed from the configuration during authentication of sessions.

  Conditions: The issue is seen when a RADIUS server is marked as dead. There are attempts to retry and access the server during its removal from the configuration.

  Workaround: There is no workaround.

- CSCsu04360

  Symptoms: Acct-Time-Delay and Tunnel-Link-Stop records are missing from L2TP network server (LNS).

  Conditions: Occurs when using radius server for authentication.

  Workaround: There is no workaround.

- CSCsu76800

  Symptoms: “Acct-Input-Giga-word” and “Acct-Output-Giga-wor” attributes are missing in the Accounting request packets.

Conditions: The symptoms are observed when you send traffic that requires the giga word counters to be incremented.

Workaround: There is no workaround.

- CSCsv02117

  Symptoms: The following system error message with "Out of IDs!" warning is seen with traceback:

  ```
  %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!) (id: 0x0)
  ```

  Conditions: This symptom is observed when flapping 24K sessions over 12K tunnel once, recreating this issue.

  Workaround: There is no workaround.

- CSCsw87061

  Symptoms: A Cisco 7304-NSE100 router crashes when configured with NAT and a large number of ACLs.

  Conditions: This symptom occurs when configuring NAT with a large number of ACLs. A malloc failure will occur and will be followed by the router crash. This happens only on NSE100 and not on NSE150.

  Workaround: There is no workaround.

- CSCsx64198

  Symptoms: Intercepted LI packets are not updated in MIB counter.

  Conditions: This symptom is observed when creating time based ACL for taps.

  Workaround: There is no workaround.

  Further Problem Description: Intercepted packet count is based on packets sent to MD. For time based ACL, it is not getting incremented although MD is receiving the packets. Due to this time based ACL script for LI, count fails.

- CSCsx73770

  Symptoms: A Cisco IOS device that receives a BGP update message and as a result of AS prepending needs to send an update downstream that would have over 255 AS hops will send an invalid formatted update. This update when received by a downstream BGP speaker triggers a NOTIFICATION back to the sender which results in the BGP session being reset.

  Conditions: This problem is seen when a Cisco IOS device receives a BGP update and due to a combination of either inbound, outbound, or both AS prepending it needs to send an update downstream that has more than 255 AS hops.

  Workaround: The workaround is to implement **bgp maxas-limit X** on the device that after prepending would need to send an update with over 255 AS hops. Since Cisco IOS limits the route-map prepending value to 10 the most that could be added is 21 AS hops (10 on ingress, 10 on egress, and 1 for normal eBGP AS hop addition). Therefore, a conservative value to configure would be 200 to prevent this condition.

- CSCsx75004

  Symptoms: In a Carriers Carrier, the CSC-PE router advertises wrong out-label. This causes the end-to-end LSP to be broken in the CSC network, and all traffic is dropped.

  This problem is observed by enabling the **show ip bgp label** command on CSC-CE. See "Out Label" of the route is "imp-null".

  Conditions: This condition is observed in routers that are running Cisco IOS Release 12.0(32)SY6.

  Workaround: Configure **neighbor** {*ip-address* | *peer- group-name*} **next-hop-self** on CSC-PE.

- CSCsx78763

  Symptoms: When deny ACL is active, packets are intercepted and is expected to be 0. However it intercepts 20 packets and sends MD and CE1 routers.

  Conditions: LI replication occurs when deny ACL is active.

  Workaround: There is no workaround.

- CSCsy09088

  Symptoms: A memory leak is seen on multiple devices.

  Conditions: This symptom occurs when policy-map type of service command and subcommands are configured.

  Workaround: There is no workaround.

- CSCsy27394

  Symptoms: Users who can execute a **show ip interface** command can see that an LI tap is in progress.

  Conditions: No specific conditions are necessary to trigger this problem.

  Workaround: There is no workaround.