Caveats for Cisco IOS Release 12.2(33)SRD through 12.2(33)SRD8

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

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

In this section, the following information is provided for each caveat:

- Symptoms—A description of what is observed when the caveat occurs.
- Conditions—The conditions under which the caveat has been known to occur.
- Workaround—Solutions, if available, to counteract the caveat.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and click **Support: Tools & Resources: Bug Toolkit** (which is listed under Troubleshooting). Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

This section consists of the following subsections:

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

Resolved Caveats—Cisco IOS Release 12.2(33)SRD8

Cisco IOS Release 12.2(33)SRD8 is a rebuild release for Cisco IOS Release 12.2(33)SRD. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRD8 but may be open in previous Cisco IOS releases.

- CSCtf71673

  Symptoms: A Cisco router shows a PRE crash.

  Conditions: This issue is seen when the system is configured for PTA and L2TP access and is running Cisco IOS Release 12.2(34)SB4 during a pilot phase.

  Workaround: There is no workaround.

- CSCtg48785

  Symptoms: The following error may appear in the log:

  ```
  %DATACORRUPTION-1-DATAINCONSISTENCY: copy error,
  ```

  Conditions: This issue occurs while issuing **show x25 hunt-group** command when a large amount of x25 traffic needs to traverse the device.

  Workaround: Do not use the **show x25 hunt-group** command.

- CSCtr28857

  A vulnerability in the Multicast Source Discovery Protocol (MSDP) implementation of Cisco IOS Software and Cisco IOS XE Software could allow a remote, unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition.

  Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-msdp

- CSCtr91106

  A vulnerability exists in the Cisco IOS Software that may allow a remote application or device to exceed its authorization level when authentication, authorization, and accounting (AAA) authorization is used. This vulnerability requires that the HTTP or HTTPS server is enabled on the Cisco IOS device.

  Products that are not running Cisco IOS Software are not vulnerable.

  Cisco has released free software updates that address these vulnerabilities.

  The HTTP server may be disabled as a workaround for the vulnerability described in this advisory.

  This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-pai

- CSCts38429

  The Cisco IOS Software Internet Key Exchange (IKE) feature contains a denial of service (DoS) vulnerability.

  Cisco has released free software updates that address this vulnerability. This advisory is available at the following link:

  http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120328-ike

Resolved Caveats—Cisco IOS Release 12.2(33)SRD7

Cisco IOS Release 12.2(33)SRD7 is a rebuild release for Cisco IOS Release 12.2(33)SRD. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRD7 but may be open in previous Cisco IOS releases.

- 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.

- CSCtg26538

  Symptoms: After applying a CoPP policy any traffic that would arrive at the CPU with an MPLS label is not classified and is classified in the class-default.

  Conditions: This symptom will be seen for any traffic arriving at the CPU with a MPLS label. The easiest manifestation of this would be to use a loopback in a VRF for management. Any traffic destined to or sourced from that loopback interface will not match the expected CoPP policy classification. For example:

```
interface loopback0
ip vrf forwarding red
ip address 192.168.1.1 255.255.255.255
!
access-list 101 permit ip any host 192.168.1.1
!
class-map  loopback-traffic
 match access-group 101
!
policy-map loopback-copp
 class loopback-traffic
  police 8000
!
control-plane
 service-policy in loopback-copp
```

Any traffic destined to the loopback0 interface will be classified in *class-default* class.

Workaround: There is no workaround.

- CSCti45732

  Symptoms: Upon a reload, a Cisco 7600 series router configured as VTP server may lose some VLANs from its VLAN database.

  Conditions: The VLANs lost do not have any access ports in the device. All other switches in the network should be in VTP transparent mode. This issue is seen on a Cisco 7600 series router that is running Cisco IOS 12.2(33)SRE1 and SRE2 Releases.

  Workaround: Configure the Cisco 7600 as VTP transparent instead of VTP server.

- CSCto43154

  Symptoms: A Cisco device running Cisco IOS may reload unexpectedly with the following message:

  ```
  %SYS-2-CHUNKBADREFCOUNT: Bad chunk reference count, chunk <address> data <address>
  refcount FFFFFFFF alloc pc <address>
  ```

  Conditions: This symptom is observed on Cisco device running Cisco IOS.

  Workaround: There is no workaround.

- CSCtq81391

  Symptoms: Standby supervisor (on a router in SSO mode) crashes upon bootup in Cisco IOS Release 12.2(33)SRD5.

  Conditions: This symptom happens when the router has multicast scale configurations, with 50+ OIFs, and 30k+ IGP routes. When active supervisor performs bulk sync, due to memory corruption issue, standby supervisor crashes.

  Workaround: Boot the router in RPR+ mode.

- CSCtr37182

  Symptoms: XAUI coding errors are seen on the console.

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

  Workaround: There is no workaround.

- CSCtr70073

  Symptoms: Multicast traffic is affected, and the PIM neighborship goes down.

  Conditions: This symptom is seen when the IPv6 address family is configured in the IPv4 MVRF.

  Workaround: Remove the IPv6 address family from the MVRF. Save the configurations and reload the router.

- CSCtr74529

  Symptoms: The following error messages are displayed:

  ```
  %ENVM-DFC3-4-LONGBUSYREAD: C2W Interface busy for long time reading temperature
  sensor 1
  %ENVM-DFC2-4-LONGBUSYREAD: C2W Interface busy for long time reading temperature
  sensor 2
  ```

  Conditions: This symptom is not caused by any specific conditions.

  Workaround: There is no workaround.

- CSCts51980

  Symptoms: STM1-SMI PAs of version 3.0 do not come up.

  Conditions: This symptom is observed when the new version of PAs do not come up with enhanced flexwan.

  Workaround: There is no workaround. Without the PA, flexwan will come up.

Resolved Caveats—Cisco IOS Release 12.2(33)SRD6

Cisco IOS Release 12.2(33)SRD6 is a rebuild release for Cisco IOS Release 12.2(33)SRD. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRD6 but may be open in previous Cisco IOS releases.

- CSCta77064

  Symptoms: Crashinfo file is not generated.

  Conditions: This symptom occurs when SIP600/ES20 line cards crash.

  Workaround: There is no workaround.

- CSCtc84960

  Symptoms: Traffic is not forwarded in LSM P2MP setup. This problem is seen after the router is booted up.

  Conditions: The problem is seen in LSM P2MP on a HA setup.

  Workaround:

  1. The problem can be prevented by configuring **tunnel mpls traffic-eng fast-reroute** on the P2MP tunnel interface.
  2. Use non HA setup.
  3. Reset the ingress line card.
  4. Program the fpoe table by using “test fpoe index *index* value *value*” or “test fpoe index *index* restore”.

  Further Problem Description: P2MP tunnels do not forward the traffic on head end after the reload because the FPOE is programmed incorrectly. Here we see the traffic hitting the tunnel interface but not the outgoing physical interface. FPOE is not getting populated due to empty port lists.

- 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.

- CSCth25634

  Symptoms: The password is prompted for twice for authentication that is falling over to the line password.

  Conditions: This symptom is observed 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 does not 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.

- CSCtj22457

  Symptoms: ISSU fails with config sync failure mcl.

  Conditions: This symptom is seen during the commitversion of ISSU.

  Workaround: There is no workaround.

- CSCtj38606

  Symptoms: The following error message is seen:

  ```
  %SYSTEM_CONTROLLER-3-MISTRAL_RESET: System Controller is reset:Normal Operation
  continues
  ```

  The **show ibc** exec command reports increments of the following counter:

  ```
  Hazard Illegal packet length = 7580
  ```

  Conditions: The symptom is observed on a Cisco 7600 series router.

  Workaround: There is no workaround.

- CSCtj53299

  Symptoms: Met corruption issue is observed.

  Conditions: This symptom occurs during OIF churn.

  Workaround: Use the **clear ip mroute** command for the problematic entry.

- CSCtj70282

  Symptoms: VRF ping does not work.

  Conditions: This symptom is seen with one or more VRFs with MDT tunnels existing on the router. In that case any application like unicast VRF, SwEoMPLS, and VPLS may be affected if they use the same VLAN.

  Workaround: There is no workaround.

- CSCtj94358

  Symptoms: SIP400 will pass the traffic through a previously configured VLAN on reconfiguring the **bridge-domain** command.

  Conditions: This symptom is seen with the egress interface that is a SIP400 with MPB configured.

  Workaround: Remove the “bridge-domain” configuration and then add the new “bridge-domain”.

- CSCtj95032

  Symptoms: PIM packets are dropped at SIP400. As a result PIM neighborship is not formed between the CEs.

  Conditions: This symptom is seen when the egress interface is on SIP400 with bridging configured on it.

  Workaround: There is no workaround.

- CSCtj96489

  Symptoms: In a CISCO 7600 router, a freshly provisioned interface, or an interface which has been administratively no shut, belonging to non-default VRF, may fail to forward traffic.

  Conditions: This is a race condition and hence timing sensitive.

  Workaround: Another interface **shut/no shut** may help restore service.

- CSCtk02155

  Symptom: Attachment to the CHOC3 SPA console fails after seeing VC configuration command failures.

  Conditions: This symptom is seen with CHOC3 SPA on SIP200 or SIP400.

  Workaround: Reset the line card.

  Further Problem Description: The periodic process resyncs the IPC between the host and CHOC3 SPA. As this is not happening, we are not able to attach to the SPA console.

- CSCtk07369

  Symptoms: The buginf statement “draco2_fastsend: PAK_BUF_ON_OBL processing vlan” appears on the console.

  Conditions: This statement is displayed in certain cases, such as multicast replication.

  Workaround: There is no workaround.

- CSCtk34380

  Symptoms: Router may crash during many additions/deletions of MVRFs and/or during SSO switchover.

  Conditions: This symptom is observed on a Cisco 7600 series router with MVRFs added/deleted in MVPN scenario.

  Workaround: There is no workaround.

- CSCtk36377

  Symptoms: VRF ping fails for some of the VRFs after deleting and adding MVRFs.

  Conditions: This symptom is seen when adding and deleting MVRFs using a script.

  Workaround: Delete VRF and add it back.

- CSCtk36897

  Symptoms: Crash is observed.

  Conditions: This symptom occurs while unconfiguring “no ipv6 mld snooping”.

  Workaround: There is no workaround.

- CSCtk47960

  Symptoms: Large CLNP packets may be dropped when forwarded over SIP- 200/Flexwan2 module. Header Syntax errors may be recorded on receiving host.

  Remote side will generate the following:

  ```
  %CLNS-3-BADPACKET: ISIS: L1 LSP, packet (902) or wire (896) length invalid
  ```

  Conditions: This symptom is seen on Cisco 7600 switch with SIP-200 line card that is running Cisco IOS 12.2(33)SRD3 and later releases.

  Issue is seen when packets larger than 911 bytes are sent (Payload and Header).

  Workaround: If CLNS is only used for ISIS neighborships “no isis hello padding” can be configured to establish ISIS neighborship. For the LSP packets, configure lns-mtu 903 under router isis on the Cisco 7600 to make this work.

- CSCtk83760

  Symptoms: Met updates from SUP are reaching Cisco 67xx DFC cards.

  Conditions: This symptom is observed during OIF churn. This is not reproduced locally, and the fix is put in as a sort of preventive mechanism.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRD5

Cisco IOS Release 12.2(33)SRD5 is a rebuild release for Cisco IOS Release 12.2(33)SRD. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRD5 but may be open in previous Cisco IOS releases.

- CSCed11719

  Symptoms: A switch is learning MAC addresses from the wrong port.

  Conditions: This symptom occurs on a dot1q trunk that is connected to that switch port with one of the subinterfaces configured for bridging.

  Workaround: There is no workaround.

- CSCsg99677

  Symptoms: Crashinfo collection to a disk filesystem will fail and generate the following error message:

  ```
  File disk#:crashinfo_20070418-172833-UTC open failed (-1): Directory entries are
  corrupted, please format the disk
  ```
  Or the crashinfo file will be stored as CRASHI~1.

  Conditions: This symptom is observed with normal crashinfo collection to a disk filesystem.

  Workaround: Configure the crashinfo collection either to a network filesystem (such as tftp or ftp) or to a local filesystem of type “flash”. Configuring to a local filesystem is a preferable option.

- CSCsk48102

  Symptoms: Supervisor crashes due to an address error on the switch processor:

  ```
  Address Error (load or instruction fetch) exception, CPU signal 10
  ```
  Conditions: This appears to be a very rare random occurrence that only occurs in devices that have uptime over one year. In some cases, the devices were up for over two years before encountering this.

  Workaround: There is no workaround.

- CSCsm97014

  Symptoms: MLPoFR with the member group interface as crackerjack PA (PA-MC-2T3-EC) is configured. On applying a simple policy along with RTP header compression virtual template, the connectivity breaks.

  Conditions: This is seen across PA (PA-MC-2T3-EC) and on applying both header compression and QoS policy.

  Workaround: There is no workaround.

- CSCso50205

  Symptoms: If a SSM static mapping command is used and router processes SSM groups outside the configured static SSM mapping range, routers fall to DNS-based look to find SSM mapping. If DNS servers are not reachable or DNS servers are not configured to provide mapping, input interface Q builds up leading to control plane instabilities affecting other protocols.

  Conditions: This symptom occurs when DNS-based SSM mapping and DNS servers are not reachable.

  Workaround: If SSM mapping information is never fetched from a DNS server, configure **no ip igmp ssm-map query dns**.

  If DNS is used, ensure that DNS servers are always reachable and also have low DNS query timeout value.

- CSCso60442

  Symptoms: A crash occurs.

  Conditions: This symptom is observed when the **show buffers interface dump** command is entered.

  Workaround: There is no workaround.

- CSCsr39340

  Symptoms: Packets may be dropped.

  Conditions: This symptom is observed if the core interface for AToM is a GRE tunnel.

  Workaround: There is no workaround.

- CSCsv70157

  Symptoms: On a Cisco 7609 router that is running Cisco IOS Release 12.2(33)SRD, after configuring any interface with any carrier-delay value other than 0 (the default), upon entering **wr mem** you get an unexpected warning message:

  ```
  "Warning: Overriding existing carrier delay value to 0"
  ```

  Conditions: There appears to be no special conditions to reproduce this defect. Simply configure any interface with a carrier delay and execute **wr mem**:

  ```
  Router#conf t
        Enter configuration commands, one per line.  End with CNTL/Z.
        Router(config)#int f2/12
        Router(config-if)#carr
        Router(config-if)#carrier-delay 2
        Router(config-if)#end
        Router#wr
        Building configuration...
        Warning: Overriding existing carrier delay value to 0

    %SYS-5-CONFIG_I: Configured from console by console[OK]
        Router#
  ```

  Workaround: There is no workaround.

  Further Problem Description: This warning should come when Asymmetric Carrier Delay (ACD) is configured on an interface and you then attempt to configure Standard Carrier Delay via the **carrier-delay** *delay* interface command. However, the message is coming when ACD is not configured.

- CSCsv73506

  Symptoms: If a port member of a Port-channel interface comes up after a service instance with bridge-domain is created, it may not join spanning tree for the VLAN corresponding to the bridge-domain.

  Conditions: Unknown at this time.

  Workaround: Perform a **shut** and **no shut** under the service instance.

- CSCsx56362

  Symptoms: BGP selects paths which are not the oldest paths for multipath. This causes BGP to unnecessarily flap from multipath to non-multipath as a result of route flaps.

  Conditions: The symptom is observed when:

  1. BGP is configured.
  2. More than one equally-good route is available.
  3. BGP is configured to use less than the maximum available number of multipaths.

  Workaround: There is no workaround.

- CSCsx78789

  Symptoms: A router crashes in the presence of MQC samplers.

  Conditions: The symptom is observed only when MQC samplers are applied to the interface, when the configurations are applied in a particular order.

  Workaround: Use NetFlow random samplers.

- 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**.

- CSCsy56433

  Symptoms: The **sh rommon rp** command for the standby intermittently fails to display the correct information for the ROMMON regions. This issue occurs intermittently and is not easily reproducible.

  Conditions: This issue was also hit during the ROMMON upgrade with Cisco IOS on standby, although this is not easily reproducible. After selecting F1 as the preferred region on the standby and resetting it, although ROMMON upgrade was successful as observed on the standby console, the **sh rommon** command on the active displays that both regions were invalid.

  The following steps provide the details that cause the reported behavior:

  1. Upgrade the standby ROMMON F1 region.
  2. Upgrade the standby F2 region.
  3. The **sh rommon** command displays that both F1 and F2 are approved, with F2 region as the preferred region. To choose the F1 as the preferred region, issue upgrade rom slot 8 rp preference region1.
  4. Then issue a HW reset to ensure that F1 region is the preferred region.
  5. As expected, the RP boots up with the upgraded ROMMON. Displays that the ROMMON is running from the F1 region.
  6. When the **sh rommon slot 8 rp** command is issued, instead of displaying F1 and F2 as approved regions, with F1 also as preferred region, the command displays that both regions are invalid, but indicates that the ROMMON is running from the F1 region.

  Workaround: There is no workaround.

- CSCsy61321

  Symptoms: Accounting requests sent to the TAC server do not fail over to the second server.

  Conditions: This symptom is observed when two TACACS servers are configured, the first without TACACS, the second with TACACS, and authentication is configured as “none”.

  Workaround: Use a single working server, or ensure that the first group uses a valid server.

- CSCsy83266

  Symptoms: A router experiences CPU hog or crashes when doing snmpwalk.

  Conditions: This symptom is observed when interfaces are attached with a large-scale police configuration (for example, a two-level policy map, 200 (parent classes) x 15 (child classes) = 3000 policers).

  Workaround: There is no workaround for walking the table. To get a specific entry, use snmpget.

- 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.

- CSCsz23099

  Symptoms: A memory leak is experienced and a higher number of loadinfo is allocated, which can be seen by using the **show ip cef loadinfo** command.

  Conditions: The symptom is observed with a router that is running Cisco IOS Release 12.2(33)SRD1 and that is configured with PBR with next-hop with reachablity that is moving between one path and two paths.

  Workaround: There is no workaround.

- CSCsz87710

  Symptoms: The RPF is enabled by default on a newly created SVI/loopback interface, which is causing ping failure. See the following example:

```
switch(config)#int vlan 1103
  switch(config-if)#mtu 9216
  switch(config-if)#ip add
  switch(config-if)#ip address 172.16.2.1 255.255.255.0
  switch(config-if)# logging event link-status
  switch(config-if)# mpls ip
  switch(config-if)#no sh

  switc#sh ip interface vlan 1103
  Vlan1103 is up, line protocol is up
    Internet address is 172.16.2.1/24
    ::: ::::::::       ::::::::::::::::::::::::
    BGP Policy Mapping is disabled
    Input features: uRPF, MCI Check   <<<<<<<<<< RPF is enabled by default
    Output features: IP Post Routing Processing, HW Shortcut Installation
    Post encapsulation features: MTU Processing, IP Protocol Output Counter,
IP
  Sendself Check, HW Shortcut Installation

  Router#ping 172.16.2.1

  Type escape sequence to abort.
  Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
  .....
  Success rate is 0 percent (0/5)
```

  Conditions: This symptom occurs when RPF is enabled on the interface for the first time. Delete the interface. Create the interface again with the same name.

  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).

- CSCta22221

  Symptoms: Frame relay client triggers reload of standby router.

  Conditions: This symptom occurs if many frame relay related configurations are present.

  Workaround: There is no workaround.

- CSCta58068

  Symptoms: During BGP convergence, a CPU spike may be seen on the local PE in an MVPN configuration.

  Conditions: The symptom may be observed with the following conditions:

  - Remote PE neighbor switchover.
  - On local PE, do a **clear ip bgp** *bgp nbr.*
  - On bring up of local PE.
  - Large configurations, such as one with 300 MDT default tunnels.

  The following is an example of an MVPN configuration where this problem can be seen:

  1. OSPF routing protocol is enabled on all the networks in the topology.
  2. Each PE router has 100 MVRFs defined (between vpn_0 to vpn_99).
  3. MDT default is configured on all the mVRFs on the PE routers.
  4. PE routers have an iBGP session, ONLY with the RR (route-reflector).
  5. eBGP session exists between the Routem and PE1, with Routem sending 200,010 VPNv4 routes.
  6. OSPF session also exists between Routem and PE1, with Routem sending 100 OSPF routes.

  In effect, the following states are present in the network:

  On PE and RR routers:

  1. IGP states = 100 OSPF routes.
  2. BGP states = 200,010 VPNv4 routes.

On PE routers ONLY:

1. VRF sessions = 100 VRFs (vpn0 to vpn_99).
2. MDT sessions = 100 SSM sessions.

Workaround: There is no workaround.

- CSCta59022

  Symptoms: On configuring auto-tunnel primary onehop and auto-tunnel backup together, the router crashes because of a stack overflow.

  Conditions: This symptom occurs when configuring mpls traffic-eng auto-tunnel and backup together

  Workaround: Configure auto-tunnel primary and wait for 10 seconds for primary to come up and then configure auto-tunnel backup.

- CSCta69118

  Symptoms: The ping from CE1 to CE2 fails when VLAN xconnect is provisioned, even though the session is up.

  Conditions: The symptom is observed with Cisco IOS Release 12.4(20)T4.

  Workaround: There is no workaround.

- CSCtb17507

  Symptoms: A crash will be seen at cfib_prefix_create_rews ().

  Conditions: This symptom occurs with high scaled configuration with multiple show and no show while installing the routes into hardware.

  Workaround: There is no workaround.

- CSCtb23840

  Symptoms: CPU HOG traceback messages may be seen when using a time-based ACL for QoS matching. The CPU hog will be printed when the time-range becomes active, or goes inactive. During the time-range active or inactive transitions, a CPU spike will be seen.

  Conditions: This symptom is seen when using a time-based ACL for QoS matching.

  Workaround: There is no workaround.

- CSCtb47647

  Symptoms: Active RP crashes at pim_send_join_prune.

  Conditions: The symptom is observed when performing some PIM-related testing with specific configurations and after carrying out an SSO. When you attempt to debug memory leak issue using a memory traceback recording command, the router crashes while executing the command **show memory traceback exclusive**.

  Workaround: There is no workaround.

- CSCtb50757

  Symptoms: The router may crash.

  Conditions: This symptom is observed when interfaces used by ISIS routers as nexthop are deleted.

  Workaround: Disable interfaces used by ISIS routes as nexthop before deleting them.

- CSCtb73450

  Symptoms: Start-Control-Connection-Request (SCCRQ) packets may cause tunnel to reset after digest failure.

Conditions: This symptom is observed when the SCCRQ packets are sent with an incorrect hash.

Workaround: There is no workaround.

- CSCtb86439

  Symptoms: Slow memory leak occurs on Cisco Intelligent Services Gateway (ISG) during normal operations.

  Conditions: Leak is observed if there is some error condition such as a mis-configuration in the user or service profile.

  Workaround: There is no workaround.

  This ddts needs to double commit to mcp_dev first, then commit to rls6. Now mcp_dev is doing some regression and scaling testing.

- CSCtb92791

  Symptoms: The command **ip ospf message-digest-key** in interface mode may have an invalid key.

  Conditions: The symptom is observed when "parser config cache interface" is configured.

  Workaround: Use the command **no parser config cache interface**.

- CSCtc27221

  Symptoms: Complete traffic that is switched through TE tunnels will be punted to RP causing high CPU and will see traffic loss.

  Conditions: This symptom is seen while testing TE-FRR.

  Workaround: There is no workaround.

- CSCtc35103

  Symptoms: ES+ switchport stops forwarding after initial configuration.

  Conditions: This symptom is seen with switchport configuration on ES+ and only sometimes.

  Workaround: Remove and reapply the configuration.

- CSCtc51539

  Symptoms: A Cisco router crashes with a "Watch Dog Timeout NMI" error message.

  Conditions: This symptom is observed only on devices configured with Bidirectional Forwarding Detection (BFD). For further information on BFD, consult the following link:

  http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/fs_bfd.html

  Workaround: Disable BFD.

- CSCtc69991

  Symptoms: A Cisco ASR 1000 Series Aggregation Services router configured as a DMVPN spoke may throw tracebacks.

  Conditions: The symptom is observed when "odr" is configured as the overlay routing protocol and a **shut** and **no shut** is done on the tunnel interface.

  Workaround: Use EIGRP as the overlay routing protocol.

- CSCtd08797

  Symptoms: MPLS packets are software switched when port-channel interfaces are the MPLS interfaces. Affects tag-to-tag traffic.

Conditions: Issue is seen after the router is upgraded to Cisco IOS Release 12.2(33)SRD3. The MTU for the MLS CEF adjacency for the MPLS label is misprogrammed and shows up as 0. Should see "MTU failures" incrementing in **show mls stat**.

Workaround: Flap the interface.

- CSCtd24840

  Symptoms: There might be collisions during switchover leading to a critical "SCP find master quiesce" message getting dropped.

  Conditions: The symptom is observed with the presence of SIP400 and 67xx cards.

  Workaround: There is no workaround.

- CSCtd38225

  Symptoms: When ISG is enabled and DHCP sessions re-start just around the time their leases expire, some sessions may get stuck dangling indefinitely. Sending DHCPDISCOVER message (i.e.: re-starting the CPE) will not restore the session. The affected subscriber(s) will not be able to establish a session.

  Conditions: The issue seems to be a corner-case situation. It is observed when ISG is enabled and DHCP sessions re-start just around the time their leases expire.

  Workaround: The only known workaround is to manually clear the dangling session(s) using the **clear ip subscriber dangling** *time* command although this may not be a suitable workaround in a live production network.

- CSCtd67010

  Symptoms: A Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRD3 may crash in process "Ethernet OAM".

  Conditions: The symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRD3. It is not necessary to have Ethernet OAM configured.

  Workaround: There is no workaround.

- CSCtd73256

  Symptoms: A Cisco Catalyst switch may reload while issuing the **show ip ospf int** command.

  Conditions: The symptom is observed when the **show ip ospf int** command is paused while the backup designated router neighbor goes down, for example:

```
c3560sw2#show ip ospf int
 Vlan804 is up, line protocol is up
   Internet Address 10.0.0.2/24, Area 0
   Process ID 1, Router ID 10.0.0.2, Network Type BROADCAST, Cost: 1
   Transmit Delay is 1 sec, State DR, Priority 1
   Designated Router (ID) 10.0.0.2, Interface address 10.0.0.2
  --More--
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/8,
 changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan804, changed
 state to down
%OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.1 on Vlan804 from FULL to DOWN,
 Neighbor Down: Interface down or detached
%LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to down
```

  The next line that will be displayed in the "show ip ospf int" output will be the following:

  Backup Designated router (ID) 10.0.0.1, Interface address 10.0.0.1

  If at this point you press enter or spacebar to advance the output, the device will reload and the following error message will be shown:

```
Unexpected exception to CPUvector 2000, PC = 261FC60
```
Workaround: There is no workaround.

- CSCtd74135

  Symptoms: Microsoft Point-to-Point Encryption (MPPE) enforcement may not work on a Cisco router. The router may allow Point-to-Point Tunneling Protocol (PPTP) users to connect without negotiating the MPPE.

  Conditions: This symptom is observed on a Cisco router that is running Cisco IOS Release 15.0(1)M even if it is configured with the **ppp encrypt mppe 128 required** command.

  Workaround: Using the authentication type of MS-CHAP in place of MS-CHAP-V2 can prevent this issue. The MPPE works fine with the required option as well, when used with the authentication type "MS-CHAP".

- CSCtd93508

  Symptoms: SIP-200 goes into crashing loop with the following messages in the log:

  ```
  %R4K_MP-3-CRASHED: CPU 1 has now crashed a total of 11 times. SYS-3-INTPRINT: Illegal
  printing attempt from interrupt level.
  -Process= "CPU Monitor", ipl= 5, pid= 54
  ```
  This secondary crash happens because of primary crash in the QoS code, which happens when high priority traffic is flowing through QoS enabled interfaces of a particular SPA.

  Conditions: From the crashed system the SPA used was "SPA-1XCHSTM1/OC3 (0x463)". Other SPAs may be affected.

  The trigger is just the flow of priority traffic through this interface with the following policy attached to that serial interface:

  ```
  policy-map child
      class pri
         priority percent 4%
      class bw
        bandwidth percent 25%
      class class-default
       bandwidth percent 71%

    policy-map parent
       classs class-default
       shape average < > kbps
       service-policy child.

  policy-map parent classs class-default shape average < > kbps service-policy child.
  ```
  Note: Any flavor of priority like priority, priority percent, priority kbps can trigger this error condition.

  Workaround: Replacing the priority percent with bandwidth percent will solve the crash, but traffic is not properly prioritized:

  ```
  policy-map child
      class pri
         bandwidth percent 4%      <<<< priority to bandwidth
      class bw
        bandwidth percent 25%
      class class-default
       bandwidth percent 71%
  ```

- CSCtd94144

  Symptoms: Ethernet OAM packets are not terminated locally.

  Conditions: This is seen only when xconnect is configured under main interface for l2tpv3 tunneling. This is not applicable for VLAN mode l2tpv3.

Workaround: There is no workaround.

- CSCte00934

  Symptoms: If configuration loss occurs after bootup due to ROMmon bug CSCsq77835, copying startup-config running-config followed by the **write memory** command does not always fix the problem.

  Conditions: This symptom is seen with corruption of SLOTCACHE ROMmon variable reenter cwan configuration-card type, controller and interface configuration write mem.

  Workaround: OIR the CWAN card, reenter cwan configuration and write memory.

- CSCte02089

  Symptoms: IP DSCP is rewritten to 0 after disposition on PE.

  Conditions: This symptom occurs when unconfiguring and adding a VRF back for packets exiting out of an interface having ip vrf receive configured.

  Workaround: There is no workaround.

- CSCte03083

  Symptoms: With queuing policy attached on MFR, removing “encapsulation frame- relay” on the physical interface puts the interface in inconsistent state. “Encapsulation frame-relay” cannot be reconfigured on the physical interface.

  Conditions: This symptom is see when QoS is in place.

  Workaround: There is no workaround.

- 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.

- CSCte10790

  Symptoms: A Cisco Catalyst 6500 series switch may unexpectedly reload due to bus error on the switching processor when making access list entry config changes or when removing an entire access-list.

  Conditions: This bug fixes two related crashes. One in which the crash occurs when making ace configuration changes and another when removing an entire ACL.

  Details on the conditions to trigger the crash when making the ace configuration changes:

  This can be reproduced in all the branches and the basic criteria reproducing this is we should have ACE is greater than 13, and we should have the extended ACE that has destination IPADDR.

  The issue is seen when we have more that three ACE which have the same source and destination address and mask and we delete the ACE in sequence like:

  no 110
  no 120
  no 130

  Then try to add ACE which has the same source address and mask but no destination. The infinite loop will result in crash.

120 ACE
130 ACE
CRASH will happen

Follow the same order:

```
ip access-list extended vlan959-out
 permit ip 10.227.128.52 0.0.0.3 any
 remark - Standard out ACL -
 permit tcp any any established
 deny   tcp any any eq 707
 deny   tcp any eq 707 any
 deny   tcp any any eq 4444
 deny   tcp any eq 4444 any
 deny   udp any any eq 31337
 deny   tcp any any eq 12345
 deny   tcp any any eq 12346
 deny   tcp any any eq 20034
 deny   tcp any any eq 7597
 deny   ip host 0.0.0.0 any
 remark - allow cns & UFAD networks
 permit ip 10.227.212.0 0.0.0.255 any
 permit ip 10.227.212.0 0.0.0.255 any
 permit ip 10.228.212.0 0.0.0.255 any
 permit ip 10.249.10.0 0.0.0.255 any
 permit ip 10.227.128.52 any
 permit ip 10.5.187.240 0.0.0.15 any
 permit ip 10.241.28.240 0.0.0.15 any
 permit ip 10.227.128.112 0.0.0.3 any
 permit udp 10.227.128.0 0.0.0.255 eq ntp 10.241.33.0 0.0.0.255
 permit udp 10.227.128.0 0.0.0.255 eq domain 10.241.33.0 0.0.0.255
 permit tcp 10.227.128.0 0.0.0.255 eq domain 10.241.33.0 0.0.0.255
 permit tcp 10.227.156.0 0.0.0.255 host 10.241.33.11 eq www
 permit tcp 10.227.128.0 0.0.0.255 host 10.241.33.29 eq cmd
```

Then follow the order:

```
no 110
no 120
no 130
120 permit udp 10.227.128.0 0.0.0.255 eq domain any
130 permit tcp 10.227.128.0 0.0.0.255 eq domain any
```

Workaround: The ACE configuration change crash can be worked around by deleting the entire ACL and then add the resequenced ACE.

The crash when removing the access-list itself has no workaround.

- CSCte38945

  Symptoms: Unable to get ping reply from the multicast group configured on loopback interface.

  Conditions: The symptom can occur when there are multiple routes populated in an interface and the interface goes down. All the routers associated with the interface should be removed, but only one is deleted. This results in the ping failure.

  Workaround: Shut down the other interfaces associated with the router and enable it again.

- CSCte48877

  Symptoms: On configuring a PVC on main interface or subinterfaces and then configuring xconnect under it, causes the standby sup to have a negative circuit id that is retained even after the switchover.

  The PVC gets a negative circuit id.

  VCs do not come up and all the xconnects are down with Cisco 7600 image. Cisco IOS Release 12.2(33)SRE has the same issue.

Conditions: See the following sample show output when this happens:

```
PE1#sh atm pvc 11/900
 ATM3/0/0: VCD: 4095, VPI: 11, VCI: 900
 UBR, PeakRate: 149760 (353208 cps)
 AAL5 L2transport, etype:0x1B, Flags: 0x1861, VCmode: 0x0, Encapsize: 4
 OAM Cell Emulation: not configured
 Interworking Method: like to like
 AC Type: ATM AAL5,  Circuit Id: -2146761852<<,  AC State: UP,  Prov: YES
 Switch Hdl: 0x1FF7FFB,  Segment hdl: 0x3FEDFF6
 AC Hdl: 0xC7010FE0,  AC Peer Hdl: 0xF4010FE1,  Flg:0,  Platform Idx:4093
 Remote Circuit Status = No Alarm, Alarm Type = None
 Local Circuit Status = No Alarm, Alarm Type = None
 InPkts: 0, OutPkts: 0, InBytes: 0, OutBytes: 0
 InPRoc: 0, OutPRoc: 0, Broadcasts: 0
 InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
 InPktDrops: 0, OutPktDrops: 0
 CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0, LengthViolation: 0,
 CPIErrors: 0
 Out CLP=1 Pkts: 0
 OAM cells received: 0
 F5 InEndloop: 0, F5 InSegloop: 0, F5 InAIS: 0, F5 InRDI: 0
 OAM cells sent: 0
 F5 OutEndloop: 0, F5 OutSegloop: 0, F5 OutAIS: 0, F5 OutRDI: 0
 OAM cell drops: 0
 Status: UP
```

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.

- CSCte49641

  Symptoms: On ES+, policy map is attached to subinterface on main or port- channel. Traffic is not being marked with CoS value specified in the policy map, and it is always propagated from dscp/precedence of the packet.

  Conditions: This symptom is seen when attaching CoS marking policy map to subinterface on main or port-channel of ES+ LC, Cisco 7600 router, enable the **mls qos** command. Traffic is not being marked with CoS value specified in the policy map, and it is always propagated from DSCP/precedence of the packet.

  Workaround: There is no workaround.

  Further Problem Description: On routed interfaces, ES+ mark the packet as “trust dscp” even when ingress marking of CoS is configured (“set cos *0-7*”) in the policy map. Because of this, CoS value is always propagated from dscp/prec.

- CSCte74705

  Symptoms: A Cisco 7600 router that is running Cisco IOS Release 12.2(33)SRD may generate L2 Queue Error (%L2-SP-4-QUEER) messages when a link down/up event occurs across multiple interfaces in a short period of time.

  Conditions: This symptom may occur when a large number of attachment circuits are configured with EVC style configuration, and a large number of MAC addresses are known to the system.

  Workaround: There is no workaround.

- CSCte78165

  Symptoms: Device may reload when the **show ip protocol** command is issued.

  Conditions: The symptom is observed when routing protocol is configured and the ISIS routes are being redistributed.

  Workaround: Do not use the **show ip protocol** command.

- CSCte79777

  Symptoms: There is a CPU hog and the router crashes.

  Conditions: The symptom is observed when the syslog is configured with a “logging discriminator”, for example:

  ```
  logging discriminator TB msg-body includes Trace
   logging trap debugging
   logging host 1.1.1.1 discriminator TB
  ```

  Workaround: Remove “discriminator” from syslog (e.g.: replacing “logging host 1.1.1.1 discriminator TB” with “logging host 1.1.1.1”).

- CSCte91656

  Symptoms: Flooding of traffic for known unicast MAC on the VPLS VCs seen after FRR cutover, reopt, or SSO switchover.

  Conditions: The symptom is observed with ES-20 as the access interfaces and having port-channel member interfaces. It is seen when you configure “ve EVC under port-channel” with bridge domain and VPLS configuration.

  Workaround: Flap the pseudowire.

- 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.

- CSCtf06442

  Symptoms: The newly active supervisor on a Cisco 7600 router with SSC-400 may crash shortly after SSO failover due to a large amount of traffic causing system instabilities.

  Conditions: This behavior is seen on a Cisco 7600 router that is running Cisco IOS Release 12.2(33)SRC5.

  Workaround: Configure MLS rate limiters to prevent RP from being overwhelmed, which may prevent the router from crashing.

- CSCtf06486

  Symptoms: SSO failover may be delayed by approximately 10 seconds when SSC- 400 is present in chassis.

  SSC-400 is not SSO aware. However other line cards may be affected by this.

  Conditions: The following error message can be seen:

  ```
  oir_enable_switching_for_modules_replied: Slot: 7 (nonEMS20g) took > 10000 ms extra to
  reply
  ```

  Workaround: There is no workaround.

- CSCtf07513

  Symptoms: A Cisco 10000 series router crashes when removing loopback interface while sessions are up and TCP traffic is flowing.

  Conditions:

  1. Reproducible under scalable scenario.
  2. Sessions should have PBHK feature.
  3. TCP traffic should be flowing.
  4. Loopback interface sourcing address to PBHK is removed.

  Workaround: Do not remove loopback interface before stopping traffic.

- CSCtf09260

  Symptoms: On a Cisco 7600 that is running Cisco IOS Release 12.2(33)SRD3 that has a Multilink PPP group configured on interfaces residing on an OSM- 1CHOC12/DS0, performing a **shut** followed by a **no shut** on the parent Multilink interface may result in the removal of a **service-policy output** command if the policy-map contains s**hape average** with a rate greater than the rate of a single Multilink PPP member link. The condition may also be triggered by the following:

  1. When you **shut** and **no shut** on the remote Multilink interface, an event that could be replayed during a telco event if all members fail.
  2. When you remove all member links either locally or on remote peer, which results in local Multilink down.

  Conditions: This issue occurs on Cisco 7600/OSM-1CHOC12/DS0 that is running Cisco IOS Release 12.2(33)SRD3.

  1. Problem does not happen if **shape average** rate is less than single_member_link_rate.
  2. Problem does not happen with a flat queueing policy attached to Multilink interface.
  3. Problem does not happen with SIP-200 and SIP-400 with various SPA modules.

  Workaround: Manually re-apply the **service-policy output** command.

- CSCtf12803

  Symptoms: The command to configure overhead accounting on an ES+ module is not available.

  Conditions: The symptom is observed with an ES+ module.

  Workaround: There is no workaround.

- CSCtf15927

  Symptoms: L2TPv3 session traffic stops flowing following an SSO failover.

  Conditions: The symptom is observed only when the local and remote end have different cookie configurations for the L2TPv3 session, followed by an SSO failover.

  Workaround: Clear the tunnel manually.

- CSCtf16623

  Symptoms: On a Cisco 7600 ES+, the internal VLAN tag is incorrectly inserted into VC-type 4 frames.

  Conditions: The symptom is observed with basic functioning.

  Workaround: There is no workaround.

- CSCtf20154

  Symptoms: Max VTemplate limit on RSP720 is 200 and cannot go beyond this number.

  Conditions: This symptom is specific to RSP720.

  Workaround: There is no workaround.

  Further Description: This limit is seen on RSP720. The limit for SUP720 is 1000.

- CSCtf22243

  Symptoms: High adjacency usage is seen in stats/non-stats region.

  Conditions: This symptom is observed when VPNV4 prefixes are getting load balanced across even number of TE Tunnels that are FRR protected.

  Workaround: Change the load-balancing mode to simple and use the **clear ip bgp neighbor *** command.

- CSCtf22968

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

  Conditions: The symptom occurs when routed pseudowire is the ingress and egress interface for multicast traffic, and an ES20+ is the exit line card. IP unicast traffic is not affected.

  Workaround: There is no workaround.

- CSCtf27303

  Symptoms: On a Cisco router, a BGP session for a 6PE (peer-enabled in AF IPv6 and end-label configured) with a third-party router, which does not advertise capability IPv6 unicast (not AFI 2 SAFI 1, only AFI 2 SAFI 4) may be torn down right after it establishes, as the Cisco router sends out an update in the non-negotiated AF IPv6 unicast (AFI/SAFI 2/1).

  Conditions: The symptom is observed under the following conditions:

  – Cisco side: session enabled for IPv6 + send-label. Cisco router is running Cisco IOS Release 12.2(33)XNE1 and Release 12.2(33)SRE.

  – Third-party: only capability IPv6 labeled unicast advertised.

  Workaround: There is no workaround.

- CSCtf29654

  Symptoms: Ingress plus egress traffic on ES-20 line card traffic is spanned. The total output traffic span destination interface is much less than aggregate traffic at ingress.

  Conditions: This symptom is seen in Cisco 7600 router having ES-20 as ingress line card and trying to monitor huge amount of traffic of more than 5 Gbps.

  Workaround: There is no workaround.

- CSCtf33203

  Symptoms: Supervisor crashes due to RPC communication failure SP-RP.

  Conditions: This symptom is observed when high temperature is seen on entire device. One module crosses alarm threshold which generates minor error RPC message.

  Workaround: There is no workaround.

- CSCtf35224

  Symptoms: When using Cisco IOS Release 12.2(33)SRD3, UDP broadcast traffic cannot be forwarded correctly through flexwan line card of the Cisco 7600. There are some count values that are increasing on serial interface of brand router, but there was no output from the **debug ip packet** command on brand router.

  Conditions: When using Cisco IOS Release 12.2(33)SRD3 based on below topology, UDP broadcast traffic cannot be forwarded correctly using the **ip helper-address x.x.x.x** command.

```
2800-4(Pagent)[F0/0] <---------> [Gi6/2] 7600-2 [S4/0/0:1] <----Serial back-
to-back-----> [S0/3/0:1] 2800-5
 Traffic Pattern from Pagent is below.
- tgn L3-src-addr 10.1.1.2
- tgn L3-dest-addr 192.168.234.255
- tgn L4-src-port 1234
- tgn L4-dest-port 1234
```

  Workaround: When using Cisco IOS Release 12.2(33)SRC1, UDP broadcast traffic can be forwarded correctly using the **ip helper-address x.x.x.x** command.

- CSCtf39455

  Symptoms: Router can hang when xconnect configuration is modified on a VLAN subinterface while data packets are being switched. The following error traceback is printed:

```
%SYS-2-NOTQ: unqueue didn't find 0 in queue
```

  Conditions: The symptom is observed when the VLAN subinterface is still seeing data traffic and the main interface is not shut down, and when the xconnect configuration on the VLAN subinterface is being modified.

  Workaround: Shut down the main ethernet interface when doing xconnect configuration changes on the subinterface.

- CSCtf44529

  Symptoms: PPPATM session does not come up on its own after switchover.

  Conditions: This symptom occurs when DLFIoATM is configured along with RPR+.

  Workaround: Use the **shutdown** command followed by the **no shutdown** command on the ATM interface.

- CSCtf48413

  Symptoms: MLS CEF entries for default route are not getting reprogrammed for default routes after a LC reload. This issue is there when default route is getting resolved through MPLS TE tunnels with FR objects, and one of the LC through which MPLS TE tunnel passes through crashes.

  Conditions: This symptom occurs when default route is reachable through more than one mpls te tunnels with FR objects. When one of the LC resets (through which MPLS TE tunnel is passing through), FR object backwalk is not fixing the adjacency properly.

  Workaround: This issue happens only in LC reset cases. This will usually not happen in customer networks. Fix by flapping the MPLS TE FRR back up tunnel.

- CSCtf50862

  Symptoms: Upon the router bootup in steady state, MAC addresses (both core and access side) are flushed out periodically resulting in traffic flooding across all ports.

  Conditions: The symptom is observed when MAC OOB is enabled by the following command: **mac-address-table synchronize**.

  If you have EVC-PC on access, VPLS in the core, and traffic flow is asymmetric, this can result in flooding of the traffic from access to core and core to access.

Workaround: Use the **clear mac-address-table dynamic** command on the RP.

- CSCtf50894

  Symptoms: During the collection process an interrupt is raised by a higher priority event (topology change, i.e.: a tunnel shutdown). If the tunnel shutdown occurs at a very precise time before the collection is complete, data structures used by FRR collection end up being deleted/altered by the higher priority event. When the suspended FRR statistics collection process resumes, it ends up working with data that has become stale/trashed. This results in a crash.

  Conditions: The symptom is observed on an MPLS TE FRR enabled router that will trigger periodic collection of accounting information for all prefixes using a given TE tunnel as its next-hop. This process is invoked in 10 second intervals and it can be suspended by other higher priority processes before its runtime completion.

  Workaround: Disable FRR protection.

- CSCtf51332

  Symptoms: An interface with PBR/VRF select configuration punts all traffic to the RP and causes high CPU usage. When MLS rate-limiter is configured, there might be packet losses at higher rate of traffic.

  Conditions: When a PBR/VRF-select route-map is removed from the first interface on which the PBR/VRF select was configured, the internal RSVD VLAN is removed. This causes the packets from all interfaces with this route-map to be punted to the RP.

  Workaround 1: Disable VPN-CAM lookup.

  Workaround 2: Configure identical route-maps with different names, for example:

```
route-map sak-vrfs-in1 permit 10
       match ip address SAK-PAM-SOURCES
       set vrf sak-pam
      !
       route-map sak-vrfs-in1 permit 20
       match ip address SAK-VOIP-SOURCES
       set vrf sak-voip
      !


       route-map sak-vrfs-in2 permit 10
        match ip address SAK-PAM-SOURCES
        set vrf sak-pam
       !
       route-map sak-vrfs-in2 permit 20
        match ip address SAK-VOIP-SOURCES
        set vrf sak-voip
       !
```

  Apply these route-maps on to the interfaces which will carry identical VRF select configurations.

```
interface GigabitEthernet2/3.104
      description SAK/PAM Turku C-FI-20709-8416
      encapsulation dot1Q 104
      ip vrf receive sak-pam
      ip vrf receive sak-voip
      ip address 10.100.220.177 255.255.255.252
      no ip redirects
      no ip proxy-arp
      ip policy route-map sak-vrfs-in1
      arp timeout 300
    !
     interface GigabitEthernet2/3.505
      description SAK/PAM Turku C-FI-20709-8416
      encapsulation dot1Q 505
```

```
 ip vrf receive sak-pam
 ip vrf receive sak-voip
 ip address 10.100.220.26 255.255.255.254
 no ip redirects
 no ip proxy-arp
 ip mtu 1500
 ip policy route-map sak-vrfs-in2
 arp timeout 300
!
```

Workaround 3: Create a dummy interface and apply this route-map first on the dummy interface (but do not delete the sub-interface).

- CSCtf51541

  Symptoms: After a parity error is detected in the system controller and a soft-reset is performed, inband traffic may be interrupted in one direction.

  The following log message indicates that the error occurred and a soft-reset was performed:

  ```
  %SYSTEM_CONTROLLER-SP-3-ERROR: Error condition detected: TM_DATA_PARITY_ERROR
  ```

  Conditions: No particular hardware or software configuration has been identified to contribute to this. The issue is due to transient hardware errors.

  Workaround: Configure EEM policy to look for the error and trigger an immediate switchover.

- CSCtf53672

  Symptoms: A router crashes when any CWAN module is not responding to the RP keepalives.

  Conditions: The symptom is observed with a Supervisor 32.

  Workaround: There is no workaround.

- CSCtf54561

  Symptoms: A MPLS TE FRR enabled router can encounter a crash if the **show ip cef vrf** *vrf-name* command is issued.

  Conditions: This symptom occurs when the VRF contains many entries (17k) in which the outgoing interface changes due to a topology change.

  Workaround: Command should not be issued when many topology changes occur on interface flaps.

- CSCtf64235

  Symptoms: Distributed LFI over ATM (dLFIoATM) session does not ping after switchover when router is configured in SSO mode.

  Conditions: The symptom is observed when the global redundancy mode is SSO.

  Workaround: Perform a **shut** and **no shut** on the ATM physical interface.

- CSCtf74073

  Symptoms: Enhanced FlexWAN resets upon copying a scaled configuration.

  Conditions: The symptom is observed upon directly copying a scaled configuration into the running configuration.

  Workaround: Copy configuration into start up from the disk or any other source file.

- CSCtf75053

  Symptoms: DHCP Relay will send a malformed DHCP-NAK packet. The malformed packet will be missing the END option (255) and the packet's length will be truncated to 300. In effect, all the options after 300 bytes, if any, will be missing.

  Conditions: When a Cisco 10000 series router is configured as a relay and a DHCP request is sent from the CPE, the router will send a DHCP-NAK when client moves into a new subnet.

Workaround: There is no workaround.

- CSCtf75587

  Symptoms: Active RP crashes when ISSU upgrade is initiated (SSO mode) from Cisco IOS Release 12.2(33)SRD3 to Release 12.2(33)SRD4.

  Conditions: The symptom is observed when “mls qos” is configured on the router and then an SSO mode ISSU switchover is initiated.

  Workaround 1: Disable QoS with the **no mls qos** command.

  Workaround 2: Upgrade in RPR mode. First, verify that following command is not in the running-configuration:

  ```
  no service image-version efsu
  ```

  If this command is in the running configuration, remove it using **service image-version efsu**.

- CSCtf77037

  Symptoms: After an OIR of Enhanced FlexWAN, some of the DLFIoATM bundles do not come up.

  Conditions: The symptom is observed after an OIR of Enhanced FlexWAN.

  Workaround: Do a shut/no shut on the ATM interface.

- 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.

- CSCtf78662

  Symptoms: On a Cisco 7600 series router that is configured with REP, the IGMP query is not forwarded through the secondary REP port leaving part of the ring incapable of receiving multicast traffic. The other switches in the REP ring located after the secondary port are unable to receive the IGMP queries from the Cisco 7600 and thus may not elect any mrouter port.

  Conditions: The symptom is observed only when the REP has a converged topology and the alternate port is not located in the Cisco 7600 but anywhere else in the REP ring.

  Workaround 1: One of the two REP ports on the Cisco 7600 must be elected/configured as an alternate port.

  Workaround 2: One of the two REP ports on the Cisco 7600 must be in shutdown.

- CSCtf79154

  Symptoms: After an SSO switchover, some of the virtual-access interfaces do not ping.

  Conditions: The symptom is observed after an SSO switchover.

  Workaround: Do a shut/no shut on the corresponding subinterface.

- CSCtf80408

  Symptoms: Enhanced FlexWAN crashes.

  Conditions: The symptom is observed with following steps:

  1. Have scaled DLFIoATM (256 bundles) on a single PA.
  2. Have traffic flowing through all the bundles.

3. Do a switchover.
4. When standby comes up, do a shut/no shut on ATM interface.

Workaround: There is no workaround.

- CSCtf82671

  Symptoms: On a 1xOC3 CEoP SPA, changing SF/SD thresholds using the **threshold sf-ber** or **threshold sd-ber** commands does not cause an APS switchover to happen at the new SF threshold.

  Conditions: The symptom is observed only if APS is enabled on a 1xOC3 CEoP SPA.

  Workaround: There is no workaround.

- CSCtf82883

  Symptoms: When clearing a VRF route, there is a traffic drop on other VRF routes.

  Conditions: The symptom is observed with an L3 VPN configuration.

  Workaround: There is no workaround.

  Further Problem Description: Some LTE broker distribution is leaked to other VRFs.

- CSCtf83737

  Symptoms: Switch Processor crashes, which can be either on the active RP or the standby.

  Conditions: This symptom occurs when IPv4 multicast routing is configured.

  Workaround: Remove multicast configuration completely.

- CSCtf84237

  Symptoms: A router may reload with the following crash decode (traceback summary):

  ```
  0x123d7e24 is in vpdn_apply_vpdn_template_pptp
  0x1239c100 is in l2x_vpdn_template_find
  0x123d81dc is in vpdn_apply_l2x_group_config
  0x123cfedc is in vpdn_mgr_call_initiate_connection
  0x123cce68 is in vpdn_mgr_event
  0x123ce974 is in vpdn_mgr_process_client_connect
  0x123cf248 is in vpdn_mgr_process_message
  0x123cf368 is in vpdn_call_manager
  ```

  Conditions: The symptom is observed when an invalid tunnel-type VSA is configured, for example:

  ```
  vsa cisco generic 1 string "vpdn:tunnel-type=l2tp_bad"
  ```

  Workaround: Configure a correct tunnel-type VSA in Radius.

- CSCtf85661

  Symptoms: Ethernet OAM packets are not punted to RP and instead are tunneled to the remote PE.

  Conditions: The symptom is observed with EoMPLS and an L2TPv3 network when “ethernet oam” is configured under the interface.

  Workaround: Configure “ethernet cfm global” in global configuration mode.

- CSCtf86240

  Symptoms: Enhanced FlexWAN with scaled DLFI setup crashes.

  Conditions: The symptom is observed with the following steps:

  1. 256 dLFIoATM interfaces on a single PA.
  2. Traffic is flowing through all the bundles.
  3. Remove IPHC configuration from all the bundles.
  4. Do a shut/no shut after removing the IPHC configuration.

5. Add IPHC configuration again and do a shut/no shut.

Workaround: There is no workaround.

- CSCtf86865

  Symptoms: Enhanced FlexWAN with scaled DLFI setup crashes on doing shut/no shut on ATM interface.

  Conditions: The symptom is observed with the following steps:

  1. 256 dLFIoATM interfaces on a single PA.
  2. 50 Mbps traffic includes 10 Mbps of 64 byte + 20 Mbps of TCP + 20 Mbps of UDP.
  3. Perform a shut/no shut on ATM interface.

  Workaround: There is no workaround.

- CSCtf90692

  Symptoms: There is an ipservices build failure due to the fix for CSCtf51332.

  Conditions: The build fails with the below compilation error:

```
const/common-rp/fm-earl7/fm_pbr_earl7.c@@ ((,),) obj-4k-draco2-mp-earl7 obj-7k-
sup3-rp-earl7 obj-m8500-sup3-rp-earl7
const/common-rp/fm-earl7/fm_pbr_earl7.c:593: relocation truncated to fit:
R_PPC_REL24 cmfi_feature_alloc_vlan_rcv_vrf
const/common-rp/fm-earl7/fm_pbr_earl7.c:593: undefined reference to
`cmfi_feature_alloc_vlan_rcv_vrf'
```

  Workaround: There is no workaround.

- CSCtf90970

  Symptoms: TX CPU might crash on a Cisco 7600 SIP-200 due to a particle chain corruption.

  Conditions: The symptom is observed when “ppp multilink interleave” is configured on a multilink PPP bundle.

  Workaround: Disable the “ppp multilink interleave” feature on the multilink PPP bundle.

- CSCtf92354

  Symptoms: Traceback is seen when doing a **shut** and **no shut** under heavy traffic (100Mbps).

  Conditions: The following steps cause this issue:

  1. 256 dLFIoATM interfaces on a single PA.
  2. Traffic is flowing through all the bundles which is above NDR (100 Mbps) but less than interface bandwidth (155Mbps). This 100 Mbps traffic includes 20 Mbps of 64 byte + 40 Mbps of TCP + 40 Mbps of UDP.
  3. Do a shut/no shut.
  4. Tracebacks will be seen.

  Workaround: There is no workaround.

- CSCtf96118

  Symptoms: A standby RSP that is supposed to start with SSO mode starts with RPR mode due to the following error.

```
Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check
full list of mismatched commands via:
  show redundancy config-sync failures mcl

Config Sync: Starting lines from MCL file:
-no mls flow ipv6
```

The running Cisco IOS image uses IPSERVICE, which is unable to configure **no mls flow ipv6**. But this command can be detected as mismatch command, and it fails to start with SSO mode.

Conditions: This issue can occur after conducting “write memory” and reloading the part.

This issue is confirmed by using Cisco IOS Release 12.2(33)SRC4. A similar issue has been seen on Cisco IOS Release 12.2(33)SRC5 and Cisco IOS Release 12.2(33)SRD4, but not on Cisco IOS Release 12.2(33)SRE.

Workaround: Conduct reload when startup-config is saved in NVRAM.

- CSCtf96659

  Symptoms: Broadcast/multicast storm across L2 switchport trunked etherchannel on ES+ links.

  Conditions: The symptom is observed with an L2 trunked port-channel interface with ES+ member links. There is “ip pim” configured on VLAN SVI where that VLAN is allowed across the trunked port-channel.

  Workaround: Use a single link configured as switchport trunk.

- CSCtg01296

  Symptoms: Enhanced FlexWAN with scaled DLFI setup resets on doing a shut/no shut on the ATM interface.

  Conditions: The symptom is observed with the following steps:

  1. 256 dLFIoATM interface on a single PA. 2. Traffic of around 44 Mbps Imix types is flowing through the all bundles. This is equally divided between all the bundles. 3. Do a continuous shut/no shut. 4. Enhanced FlexWAN might reset. It does not generate a crashinfo.

  Workaround: There is no workaround.

- CSCtg11217

  Symptoms: Standby crashes when doing an SSO.

  Conditions: The symptom is observed when one of the slots in the chassis has a fabric connection issue.

  Workaround: Power down the module in the slot that is having the fabric connection issue.

- CSCtg11421

  Symptoms: The following issues are observed:

  – All egress traffic by SIP-400 is dropped.
  – Consecutive BusConnectivityTest failure for SIP-400.
  – When SIP-400 is hosting intelligent SPAs such as SPA-8XCHT1/E1, then this SPA gets into OutSrvc state.

  Conditions: The symptom is observed with a SIP-400 with egress LLQ shaping and with a high volume of traffic to low speed stream.

  Workaround 1: SIP-400 reload using the **hw-module module X reset** command (where X is the module/SIP-400 number).

  Workaround 2: Remove LLQ configuration.

  Workaround 3: SIP-400 microcode reload (where X is the module/SIP-400 number):

```
attach X
enable
microcode reload np
```

- CSCtg13413

  Symptoms: ESP tunnel establishment with VPNLB is unsuccessful.

  Conditions: The symptom is observed with ESP VServer and UDP VServer with ISAKMP configured in a basic hub-spoke VPN setup.

  Workaround: There is no workaround.

- CSCtg14446

  Symptoms: Packets are dropped in excess of the configured rate for hierarchical policies, with shaper in the parent policy.

  Conditions: The symptom is observed only with HQoS policies (flat policies are not affected).

  Workaround: There is no workaround.

- CSCtg14755

  Symptoms: In a 6PE environment, on a Cisco 7600 PE injecting a directly connected v6 prefix, the hardware programming for the BGP local label for that prefix might be incorrect when an IPv6 address is deleted and re-added.

  Conditions: The symptom is observed when multiple BGP paths exist for this prefix (remote PEs advertise the same prefix).

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

- CSCtg16191

  Symptoms: A SIP-400 line card may crash due to a memory leak in the code for bringing down PPPoE sessions. A few hours before the crash, the line card starts to generate the following logs:

  ```
  %SYS-2-MALLOCFAIL: Memory allocation of
  100352 bytes failed from 0x407F181C, alignment 0
  Pool: Processor  Free: 2242304  Cause: Memory fragmentation Alternate Pool:
  None  Free: 0  Cause: No Alternate pool
  ```

  You can also verify this memory leak using the **show memory allocating-process totals** command on the SIP-400 line card and searching for VA_LOCK. More memory is allocated to VA_LOCK when you bring up PPPoE sessions, but the usage will not go down even after the PPPoE sessions are torn down.

  Conditions: The symptom is observed only with PPPoE sessions.

  Workaround: There is no workaround.

- CSCtg22774

  Symptoms: The input queue on which the packets are being received for RLB is getting wedged and all the packets are being dropped.

  Conditions: The symptom is observed on an RSP720 platform only and when the packet size is more than 512 bytes.

  Workaround: You can use SUP720, if the hardware is available.

  Further Problem Description: RSP platform supports particle-based packet buffers. When the packet is punted to the SLB process, the particles are collated and converted to contiguous buffers. If there is an error in the RLB packet processing, then the packet is being freed assuming that it is a particle. This freeing is not succeeding and the packet is getting queued to the input interface queue permanently.

- CSCtg35298

  Symptoms: Traffic drops are seen between two PEs after re-optimization.

Conditions: The symptom is observed with 16k VPLS VC, 4k scalable EoMPLS, 1K software EoMPLS, 600 primary tunnels to nPE1 and one tunnel to nPE2 from nPE3.

Workaround: There is no workaround.

- CSCtg44996

  Symptoms: Flows get dropped when the packet size is greater than 1514.

  Conditions: The symptom is observed after L2TPv3 reassembly on an ES+ card with default MTU on access facing. The packets get dropped because of MTU validation. This is seen in VLAN mode configuration only.

  Workaround: Increase the access facing MTU.

- CSCtg49331

  Symptoms: Multicast streams may not be forwarded to some interfaces, even though they are forwarded to other interfaces on the device without issues.

  Conditions: The symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRD4 with egress multicast replication mode.

  Workaround: Use ingress replication mode. If egress replication mode is used and the issue is present, service can be restored by using the **clear ip mroute** *A.B.C.D* command:

  Or perform a **shut** and **no shut** on the affected interface.

- CSCtg52130

  Symptoms: When running “show mmls met” on SP or DFC, the line card crashes

  Conditions: This symptom will happen when the met set has a fixed set.

  Workaround: There is no workaround.

- CSCtg62555

  Symptoms: System may be out of service after removing the IP address from the “ip portbundle source loopback” interface. The following error may be shown:

```
%SYS-2-CHUNKFREE: Attempted to free nonchunk memory, chunk 2BA721819088,
 data 2BA760900868. -Process= "SSM connection manager", ipl= 0, pid= 137
 -Traceback= 1#cdb5a75db2833d1c207cda33ef68fc00  :400000+6D755D :400000+1AF0949
 :400000+49D5A2B
 :400000+49D98FF :400000+49DB212 :400000+1919497 :400000+19044BF :400000+190434B
 :400000+18FA668
 :400000+18F9378

 %Software-forced reload
```

  Conditions: This symptom is observed on a Cisco ASR1000 series router functioning as an ISG, when Port Bundle Host Key (PBHK) is enabled on the sessions, when thousands of sessions are established, and a high rate of traffic is running in both the upstream and downstream directions.

  Workaround: There is no workaround.

- CSCtg73456

  Symptoms: Bulk sync fails due to applying the **tx-ring- limit** command on the main interface, which is not supported.

  Conditions: This symptom occurs when appling the **tx-ring- limit** command on the main interface and doing an SSO.

  Workaround: There is no workaround.

- CSCtg83578

  Symptoms: When you disable and enable the **mls qos rewrite ip dscp** command, the set functionality is not working.

  Conditions: The symptom is observed with a policy-map with set operation, and when you execute the **no mls qos rewrite ip dscp** and **mls qos rewrite ip dscp** in the global mode.

  Workaround: Execute **no mls qos** and **mls qos** in the global config mode.

- CSCtg91201

  Symptoms: DHCP-added static routes get removed sometimes and the traffic towards the host gets dropped.

  Conditions: The symptom is observed with IP unnumbered relay and with a third party external DHCP server. (This issue can also occur with an IOS DHCP server, but the probability is quite low.)

  Workaround: There is no workaround.

- CSCtg92587

  None High CPU in the SNMP Engine process is observed every five minutes.

- CSCtg94250

  Symptoms: Removing **address-family ipv4 vrf** *vrf* (in router BGP) followed by **no ip vrf** *vrf* (where "vrf" is the same) could result in a crash.

  Conditions: The symptom is observed in a large VPNv4 scale setup, when applying the following commands to the same VRF back-to-back:

  1. **no address-family ipv4 vrf** *vrf*
  2. **no ip vrf** *vrf*
  3. **ip vrf** *vrf*

  The trigger of the BGP crash is a result of a racing condition between event 1 and event 2.

  Workaround: Since this is a racing condition, the workarounds are:

  1. Not applying (1) before (2).
  2. Give sufficient time for (1) to complete before applying (2).

- CSCth01394

  Symptoms: On a Cisco 7606 router that is running Cisco IOS Release 12.2(33) SRD3 with SIP200/SPA-4XCT3/DS0, when you have ppp multilink interface(s) configured with member links from same SPA (software based multilink) and you physically remove SPA, you will see that upon executing the **show ppp multilink** command, the multilink interface still has reference for member links. If you do the **sh run int serialx/y** command, you will get message interface not found.

  Conditions: This issue is consistently reproducible.

  Workaround: There is no workaround.

- CSCth02479

  Symptoms: Router crashes.

  Conditions: The symptom is observed when the **show upgrade fpd file** *tftp:* command is performed.

  Workaround: Copy the fpd file to "disk:" and then perform the **show upgrade fpd file** *disk:* command.

- CSCth02725

  Symptoms: There is an interoperability issue between a third-party vendor's routers and Cisco routers with severe IPTV service failure in Prune-Overriding environment.

  Conditions: The symptom is observed in the following scenario:

  1. Router A is Cisco 7609 router (IP address 10.1.1.1) and connects to Router B (third-party vendor's router; IP address 10.1.1.3) and Router C (IP address 10.1.1.2).
  2. If subscriber under Router C disappears, Router A receives "Prune" message from Router C.
  3. Router A does not change "source IP of PruneEcho message (10.1.1.2)" and sends it to Router B.
  4. At this time, Router B should send overriding-join to Router A because Router B still has subscribers. But Router B drops the PruneEcho message because source IP (10.1.1.2) is not from PIM neighbor. Router B cannot send overriding-join to Router A.
  5. As a result, multicast traffic (IPTV stream) to Router B stops.

  Workaround: Connect C and B to become PIM neighbors. However, this cannot always be considered a recommended workaround because of potential high cost and/or other (sometimes third-party) limitations.

- CSCth15790

  Symptoms: ES+ low-queue line card crashes with HQoS policy applied.

  Conditions: The symptom is observed with an HQoS policy and with three-level HQoS and classes containing "priority" statements for either priority level1 or level2. When traffic passed through either of the PQ classes the line card may crash after some random period of time.

  Workaround: There is no workaround.

- CSCth18571

  Symptoms: An ES+ module may reload when a SPAN session is configured for a source VLAN.

  Conditions: The symptom is observed with a Cisco 7600 ES+ and with Cisco IOS Release 12.2(33)SRD4. VFI configuration needs to be present.

  Workaround: There is no workaround.

- CSCth33500

  Symptoms: NAS port is reported as zero on LNS.

  Conditions: This symptom occurs when "vpdn aaa attribute nas-port vpdn-nas" is configured.

  Workaround: There is no workaround.

- CSCth46888

  Symptoms: When ARP entry is refreshed due to timeout or execute **clear arp** command, router sends ARP request for cached MAC address. However, request message does not use virtual MAC for Source (Sender) MAC.

  Conditions: This symptom occurs when the router is VRRP master, and VRRP IP is configured the same as the interface IP.

  Workaround: There is no workaround.

- CSCth55383

  Symptoms: When entering the **show tech** command on RP, the line card with DFC may display SWITCH_BUS_IDLE message.

  Conditions: This symptom occurs when entering the **show tech** command on RP.

Workaround: There is no workaround.

- CSCth64439

  Symptoms: With different image versions and with “issu image-version comp disable” configured, the standby comes up in SSO mode instead of RPR.

  Conditions: The symptom is observed when “issu image-version comp disable” is configured.

  Workaround: Enable image-version compatibility check (using **issu image-version comp enable**).

- CSCth66700

  Symptoms: (S,G) expiry timer is updated again about two minutes after stopping the (S,G) stream.

  Conditions: The symptom is observed with the (S,G) expiry timer.

  Workaround: There is no workaround.

  Further Problem Description: The behavior of the expiry timer is not changed even if you change the value of **mls ip muticast flow-stat-timer**.

- CSCth69504

  Symptoms: A Cisco 7600 series router may experience a small buffer leak in the small buffer pool on SP.

  Conditions: The symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRD configured with IGMP snooping.

  Workaround: Disable IGMP snooping either globally or per VLAN.

- CSCth71899

  Symptoms: An SSO causes a met3 VLAN to become 0.

  Conditions: The symptom is observed with 600 S,G distributed with OIFs over SVIs and L3 interfaces and after an SSO. It happens only on triggering joins and leaves for the groups, on the CFC card.

  Workaround: There is no workaround.

- CSCth72565

  Symptoms: The reachability of the PE2 router’s loopback is lost from PE1 after an interface flap in the core. The LSP toward PE2 “breaks” due to data plane programing error (wrong labels).

  Conditions: The symptom is observed with MPLS with the presence of ECMP. The PE1 has two uplinks to core routers. In a steady state there is no ECMP between PE1 and PE2. When a link is lost in the P-core (link flap or **shut** and **no shut**) there is ECMP between PE1 and PE2. After the link flap between the two P routers in the core, PE1 is losing connectivity to PE2.

  Workaround 1: Use the **clear ip route** on the affected IP address.

  Workaround 2: Avoid ECMP by altering link cost.

- CSCth72765

  Symptoms: Configuring “mls qos protocol hsrp police *rate*” does not enable policing of HSRPv2 packets.

  Conditions: The symptom is observed on a Cisco 7600 series router when “mls qos protocol hsrp police *rate*” is configured.

  Workaround: There is no workaround.

- CSCth84995

  Symptoms: Router may reload when performing an ISSU upgrade or downgrade.

Conditions: This symptom occurs when performing an ISSU upgrade or downgrade.

Workaround: There is no workaround.

- CSCth87195

  Symptoms: Flexwan ATM interface goes down.

  Conditions: This symptom is observed while configuring “mac-address” or “atm bridge-enable”.

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

- CSCth90001

  Symptoms: Packets egressing interfaces of ES+ line cards are not received on the other side of L2 link when SVI plus switchport configuration is used. It is random and does not occur on every ES+ line card.

  Conditions: This symptom is observed when ES+ line card is egress line card and SVI plus L2 switchport configuration is used. When this issue is seen the CFI bit in vlan tag header for such packets is set by X40g egress-intf causing the peer router to drop such packets.

  Workaround: Use L3 802.1q subinterface configuration.

- CSCti00020

  Symptoms: Standby takes more time to come up on SSO.

  Conditions: This symptom depends on the SIP based cards that are on the chassis. Every single SIP based card increases the time by one more minute.

  Workaround: There is no workaround.

- CSCti14290

  Symptoms: A Cisco 7600 series router acting as the PE router in an MPLS network may stop forwarding traffic for certain IP prefixes within a VRF. This symptom may occur after a router reload, upgrade or crash due to corrupted hardware-forwarding information on the ingress module for the VPN label of the affected IP prefix.

  The problem can be identified by comparing the output of the following commands:

  1. Determine the BGP VPN Label for the prefix

     show ip bgp vpnv4 all vrf *vrf name* **prefix**

     ```
     router# sh ip cef vrf test 10.1.1.1 detail
     10.1.1.0/24, epoch 13
       local label info: other/4828 <=== label is 4828
       recursive via 10.100.1.2
         attached to GigabitEthernet1/1
     ```

  2. Determine the hardware forwarding for the prefix on the Supervisor

     show mls cef mpls label *label* **detail**

     ```
     RCORL02#sh mls cef mpls label 4828 detail

     Codes: M - mask entry, V - value entry, A - adjacency index, P - FIB Priority
            D - FIB Don't short-cut, m - mod-num, E - ELSP?
     Format: MPLS - (b | xtag vpn pi cr mcast label1 exp1 eos1 valid2 label2 exp2
     eos2)
     V(2570   ): B | 1 0    0 0 0 4828    0 1 0 0       0 0
     (A:213683 ,P:0,D:0,m:0 :E:1)
     M(2570   ): F | 1 FFF  0 0 1 FFFFF   0 1 0 0       0 0
     ```

     show mls cef adjacency entry *entry id*

```
DRCORL02#sh mls cef adjacency entry 213683 detail

Index: 213683  smac: 0000.0000.0000, dmac: 00d0.2b12.5500
               mtu: 65535, vlan: 1024, dindex: 0x7FFA, l3rw_vld: 1
               format: MPLS, flags: 0x1000008600
               label0: 0, exp: 0, ovr: 0
               label1: 0, exp: 0, ovr: 0
               label2: 0, exp: 0, ovr: 0
               op: POP
               packets: 0, bytes: 0
```

3. attach to the ingress module and use the same commands as step 2 and compare the values, if the destination mac address is not the same there is hardware forwarding corruption. Note: The adjacency index will be a different number on the module dfc.

remote login module *module number*

```
Router# remote login module 1
Trying Switch ...
Entering CONSOLE for Switch
Type "^C^C^C" to end this session


Router-dfc1#sh mls cef mpls label 4828 detail
Codes: M - mask entry, V - value entry, A - adjacency index, P - FIB Priority
       D - FIB Don't short-cut, m - mod-num, E - ELSP?
Format: MPLS - (b | xtag vpn pi cr mcast label1 exp1 eos1 valid2 label2 exp2
eos2)
V(1301   ): B | 1 0    0 0 0 4828    0 1 0 0       0 0
(A:147570 ,P:0,D:0,m:0 :E:1)
M(1301   ): F | 1 FFF  0 0 1 FFFFF   0 1 0 0

      0 0
Router-dfc1#sh mls cef adjacency entry 147570 detail
Index: 147570  smac: 0000.0000.0000, dmac: 0000.138b.0000
               mtu: 65535, vlan: 1024, dindex: 0x7FFA, l3rw_vld: 1
               format: MPLS, flags: 0x1000008600
               label0: 0, exp: 0, ovr: 0
               label1: 0, exp: 0, ovr: 0
               label2: 0, exp: 0, ovr: 0
               op: POP
               packets: 59, bytes: 24025
```

Conditions: The Cisco 7600 must have a distributed forwarding card installed on the ingress module and be configured as an MPLS PE router. The problem is only observed after a router reload, upgrade, or crash.

Workaround: Reloading the ingress module will resolve the hardware forwarding corruption on the module:

hw-module module *module number* **reset**

- CSCti24657

  Symptoms: New settings for fabric channel preemphasis are for sip600/esm20 card for Cisco 7609, Cisco 7609S, and Cisco 7613 chassis.

  Conditions: There are no conditions.

  Workaround: There is no workaround.

- CSCti37167

  Symptoms: A router crashes.

  Conditions: This symptom occurs after router compares the snmp value of mplsTunnelLastPathChange.

Workaround: There is no workaround.

- CSCti37503

  Symptoms: RP is dropping IPv6 mcast packet.

  Conditions: This symptom happens while sending to SSM group.

  Workaround: There is no workaround.

- CSCti68153

  Symptoms: QinQ packet header is modified breaking QinQ.

  Conditions: This symptom occurs when you use ES+ card on the Cisco 7600 where the pseudowire encapsulation begins.

  Workaround: One possible workaround is to use double vlan tagging before the packet gets to the ES+ card so that when it pops the first Vlan tag, it will modify the second dummy tag and not the actual Payload. This issue is also not seen on ES20 card.

- CSCti80956

  Symptoms: Traffic outage and duplication is seen during fibre cut in customer deployment.

  Conditions: This symptom is seen with traffic reroute, L2/L3 co-existence.

  Workaround: There is no workaround.

- CSCtj08597

  Symptoms: With the following simple topology, the router crashes when sending IGMP joins from IXIA:

  UUT-----Peer-----Ixia

  The peer is a Cisco 7600 router acting as a layer2 (only switchport config towards UUT and IXIA) box. There are 10 OIF interfaces on UUT.

  Conditions: This symptom is observed when doing a SSO switchover.

  Workaround: There is no workaround.

- CSCtj15265

  Symptoms: The event trace buffer gets wrapped around resulting in met cc log not being available.

  Conditions: This symptom is seen when there is a lot of OIF churn.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRD4

Cisco IOS Release 12.2(33)SRD4 is a rebuild release for Cisco IOS Release 12.2(33)SRD. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRD4 but may be open in previous Cisco IOS releases.

- CSCee36959

  Symptoms: A Cisco 6500 and Cisco 7600 may rarely and unexpectedly reload with the following error message on the SUP:

  ```
  %RPC-SP-2-FAILED: Failed to send RPC request
  online_diag_sp_request:get_rp_cpu_info.
  ```

  Conditions: This occurs very rarely when the MSFC or RP is too busy processing an event and can not respond to the RPC from the SUP. This is seen only on systems that run native Cisco IOS.

Workaround: There is no workaround.

- CSCek48205

  Symptoms: The output counters for a Multilink Frame Relay (MFR) bundle interface may not be updated correctly.

  Conditions: Occurs after the same interface is deleted and recreated.

  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.

- CSCsc85962

  Symptoms: When retransmitted packet of Main Mode is received at Cisco IOS router after established SA, it deletes its IKE SA.

  Conditions: Replayed packet of Phase 1 is resent.

  Workaround: There is no workaround.

- CSCsh79241

  Symptoms:

  1. Tracebacks are occasionally seen when the action “Limit+flood” is triggered.
  2. Tracebacks are seen when the “Limit+flood” action is triggered and the MAC limit for the VLAN is removed.

  Conditions: The symptom is observed when DFCs are present in the chassis.

  Workaround: There is no workaround.

- CSCsi51649

  Symptoms: A device may reload with NAT traffic under certain conditions.

  Conditions: The symptom may be seen in rare cases if a number of successive packets of the same flow are received at a high rate and the pool memory is exhausted in the software.

  Workaround: There is no workaround.

- CSCsi97428

  Symptoms: SSM (S,G) entries periodically created and deleted if OIL is Null and if source is not directly connected.

  Conditions: Issue observed on Cisco 7600 platform running Cisco IOS Release 12.2(33)SRC4.

  Workaround: There is no workaround.

- 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.

- CSCso86544

  Symptoms: After an SSO the new active SP crashes at pm_vlan_get_portlist.

  Conditions: The symptom is observed after an SSO and is triggered by an OIR offline.

  Workaround: There is no workaround.

- CSCsq11897

  Symptoms: A crash is seen when the interface board is removed.

  Conditions: The symptom is observed in a very rare scenario when a BGP session is established and the corresponding interface board is removed.

  Workaround: There is no workaround.

- CSCsq68156

  Symptoms: FRF12 packets are dropped by a PE router.

  Conditions: This symptom is observed on a Cisco 12000 series Internet router that has a SPA-1XCHSTM1/OC3, SPA-2XCT3/DS0, or SPA-8XCHT1/E1.

  Workaround: There is no workaround.

- CSCsq82663

  Symptoms: Very high CPU utilization observed under a ~400 MB traffic load on a Cisco Catalyst 6503-E or 6504-E switch with the Cisco IOS Server Load Balancing (SLB) feature.

  Conditions: The symptom is observed when the SLB feature is deployed on a Cisco Catalyst 6503-E or 6504-E switch, for DMVPN hubs load balancing for branches (spokes) using OC12 POS SPA as the WAN interface. When traffic is sent from the branch to the networks behind hubs, SLB is not able to install the shortcuts for hardware switching for ingress POS WAN port. The packets are process switched, which increases CPU usage dramatically.

  Workaround: There is no workaround.

- CSCsq83789

  Symptoms: Some L3 interfaces have the wrong LTL programmed for Unknown Unicast.

  Conditions: The symptom is observed in a chassis with a SPA-IPSEC-2G card.

  Workaround: There is no workaround.

- CSCsr47527

  Symptoms: The following errors will prevent a standby processor from reaching Hot Standby (full SSO).

  ```
  Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check full
  list of mismatched commands via: show redundancy config-sync failures mcl
  Config Sync: Starting lines from MCL file: -
  ```

  Conditions: This symptom is most often seen during an ISSU upgrade.

  Workaround:

  1. Let the Standby come up in RPR mode after MCL mismatch.
  2. Then apply the **redundancy config-sync ignore mismatched-commands** command in exec mode on Active.
  3. Now change the redundancy mode to SSO on Active. The setup will come up in SSO mode.

- CSCsr64777

  Symptoms: A router crashes because of a block overrun (overwriting the memory block).

  Conditions: This symptom is observed only when NetFlow version 5 is used.

  Workaround: NetFlow version 9 could be used for exporting.

- CSCsr72674

  Symptoms: There is a possibility the RP could encounter a software exception, resulting in a crash.

  Conditions: The symptom is observed with MPLS VPN enabled over a tunnel (GRE, for example) and when the tunnel is configured to be associated with a user-configured VRF.

  Workaround: There is no workaround.

- CSCsu04049

  Symptoms: Following an SSO, pruning recalculations are not done on the new active supervisor and all the VLANs that are available on the switch are put into a not-pruned list.

  Conditions: The symptom is observed following an SSO on the new active supervisor.

  Workaround: There is no workaround.

  Further Problem Description: The join messages from the peer are not handled because flag clearing after the VLAN addition is not occurring on the standby. Thus, after the standby becomes active, the pruning recalculations do not occur.

- CSCsu45210

  Symptoms: After upgrading from Cisco IOS Release 12.2(18)SXF8 to 12.2(33)SXH2, the standby supervisor constantly reloads with no error messages.

  Conditions: The symptom is observed after a software upgrade using the standby. The standby is reloaded with the new software, there is a switchover, then the standby is reloaded again.

  Workaround: Remove the port security configuration on all ports.

- CSCsu46644

  Symptoms: After the router reboots, the username/password prompt does not appear after three minutes. The following message is shown instead of the router login prompt:

  ```
  % Authentication failed
  ```

  Conditions: The symptom is observed on a router that is running Cisco IOS interim Release 12.2(33.1.18)SB1.

  Workaround: Add the “no no aaa account system guarantee-first” configuration.

- CSCsu59900

  Symptoms: Standby RP crashes.

  Conditions: Occurs when a **shut/no shut** is performed on the subinterface with a anything over MPLS (AToM) VP configured.

  Workaround: There is no workaround.

- CSCsu76993

  Symptoms: EIGRP routes are not tagged with matching distribute-list source of route-map.

  Conditions: Problem is observed where the route-map is applied to a specific interface. When the route-map is applied globally without the specific interface things appear to work fine.

  Workaround: There is no workaround.

- CSCsu89656

  Symptoms: A router may reload when a user reconfigures ATM AToM VP.

  Conditions: There is slim timing window that the router may reload when a user issues the commands to reconfigure the ATM VP.

  Workaround: There is no workaround.

- CSCsu92300

  Symptoms: After the IP address of the loopback interface at the PE router is changed, some Mroute entries are in a pruned state.

  Conditions: The symptom is observed after changing the IP address of the loopback interface which is configured as the source interface for an MDT tunnel.

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

- CSCsu96698

  Symptoms: More specific routes are advertised and withdrawn later even if **config aggregate-address net mask summary-only** is configured. The BGP table shows the specific prefixes as suppressed with s>

  Conditions: This occurs only with very large configurations.

  Workaround: Configure a distribute-list in BGP process that denies all of the aggregation child routes.

- CSCsu99270

  Symptoms: A Cisco Catalyst 6500 system running with VPNSPA in crypto-connect mode may see high CPU utilization on the RP. Generally, high CPU will be associated with the ARP input process.

  Conditions: The symptom will be seen when the VPNSPA is configured to be in crypto-connect mode.

  Workaround: There is no workaround.

  Further Problem Description: The problem can be verified by running the command **show crypto vlan**, noting down the port-VLAN (for example: Vlan 710, hex 2C6), logging into the switch **remote log switch** and running the command **test mcast ltl index Cxxx**, where xxx is the hex-value of the port-VLAN (in this case, C2C6).

  If the command shows the RP as part of this LTL index and there is high CPU utilization then it is possible that you are hitting this issue. If this issue is suspected then you should also determine what packets are hitting the route-processor.

- CSCsv09467

  Symptoms: Router crashes when interface is defaulted with port-security sticky MAC address configured.

  Conditions: The symptom is observed under the following conditions:

  1. On a router that is running Cisco IOS Release 12.2(33)SRD.
  2. . “Switchport” is configured with port-security and sticky MAC address:

```
interface <>
    switchport
    switchport mode access
    switchport access vlan <>
    switchport port-security
    switchport port-security mac-address sticky
```

3. With traffic on, interface mode is changed as follows:

   a. access mode to trunk mode

   b. trunk mode to access mode

4. Default the interface with “default int <>” from configuration mode.
5. Router crashes.

Workaround: There is no workaround.

Further Problem Description: Mode changes on switchport with port-security configured from access mode to trunk mode and then to L3 port by defaulting the interface configuration (with the **default interface** *interface-number* command) in configuration mode can cause the router to crash.

- CSCsv18579

  Symptoms: The logging buffer fills with this message:

  UTC: FC1: recognized & transferred a satvcl packet, total 604369 UTC: DFC1: recognized & transferred a satvcl packet, total 604370 UTC: DFC1: recognized & transferred a satvcl packet, total 604371 UTC: DFC1: recognized & transferred a satvcl packet, total 604372 UTC: DFC1: recognized & transferred a satvcl packet, total 604373

  Note: The counter always increments by one.

  Conditions: The symptom is observed with Cisco IOS Release 12.2(18)SXF5 and when reflexive ACL is configured.

  Workaround: There is no workaround.

- CSCsv49924

  Symptoms: The wrong binding and route are created on the DHCP Relay Agent.

  Conditions: The symptom is observed when multiple DHCP Relay Agents are present in between clients and the DHCP server.

  Workaround: There is no workaround.

- CSCsv66694

  Symptoms: If the router has a static route and that route is redistributed into EIGRP with a route-map, the EIGRP topology table shows that the router is setting the tag on the redistributed route. However, both the routing table and the EIGRP topology table do not show the tag as being set.

  Conditions: The symptom is observed when a Cisco ASR 1006 router that is running Cisco IOS Release 12.2(33)XNB1 is EIGRP neighbors with a Cisco 7300 series router (running Cisco IOS Release 12.2(31)SB10).

  Workaround: There is no workaround.

- CSCsv81952

  Symptoms: Standby supervisor reloads due to parser return code error.

  Conditions: The symptom is observed when the redundant supervisor is running Cisco IOS Release 12.2(33)SRD3.

  Workaround: There is no workaround.

  Further Problem Description: The issue can be seen, for example, by creating parser view (it was also reported when removing service policy from ATM subinterface):

  ```
  Router#conf t
  ```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#parser view CDandA
%PARSER-6-VIEW_CREATED: view 'CDandA' successfully created.
Router(config-view)#
%RF-SP-5-RF_RELOAD: Peer reload. Reason: Proxy request to reload peer
%OIR-SP-3-PWRCYCLE: Card in module 8, is being power-cycled (RF request)
%PFREDUN-SP-6-ACTIVE: Standby processor removed or reloaded, changing to
Simplex mode
Router(config-view)#
```

- CSCsw81427

  Symptoms: Label entries in the TCAM are leaking when there is label deallocation, due to routing or LDP events.

  Conditions: The symptom is observed when LDP or BGP withdraw labels due to network events like a route flap or link flap.

  Workaround: There is no workaround.

  Further Problem Description: Labels in the hardware are not deleted when the labels are withdrawn by LDP or BGP. This can cause traffic loss or traffic misforwarding if those labels are again installed by LDP or BGP.

- CSCsx10028

  Symptoms: A core dump may fail to write or write very slowly (less than 10KB per second).

  Conditions: The symptom is observed when the cause of the crash is processor memory corruption. When this occurs, the corrupted memory pool cannot be used to write the core dump so it will likely fail. (IO memory corruption crashes should not have this problem.)

  Workaround: There is no workaround.

- CSCsx16206

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

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

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

- CSCsx20177

  Symptoms: “no int loopback” with “advertise passive-only” causes a stuck prefix.

  Conditions: This symptom is observed on a Cisco 7600 series router that is using an RSP720 with Cisco IOS Release 12.2(33)SRD.

  Workaround:

  – Do not use “advertise passive-only”. Unconfiguring and reconfiguring this command clears the stuck prefix.

  Or with “advertise passive-only”:

  – First remove “passive-interface loopback” from router isis.

  - Then remove the interface via “no int loopback”.

- CSCsx20659

  Symptoms: There is a ping failure on an ES-20 line card.

  Conditions: The symptom is observed when booting while the ICC mechanism is busy.

  Workaround: Perform a shut/no shut on the interface, after booting up.

- 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.

- CSCsx39263

  Symptoms: After an SSO, TCP Intercept entries in TCAM are not programmed correctly. As a result, TCP packets are not punted to software and thus Netflow entries are not installed.

  Conditions: The symptom is observed when TCP Intercept is already configured when the standby comes up. Also, at least two switchport interfaces are present in the router.

  Workaround: Remove the TCP Intercept configuration and then reconfigure it.

- CSCsx46854

  Symptoms: Tracebacks are seen from the interrupt scheduler due to a process suspension.

  Conditions: The symptom is observed when changing the IMA group and trying to remove the ATM/IMA interface.

  Workaround: There is no workaround.

- CSCsx55672

  Symptoms: Client fails to get an IP address when it sends a subscription request to the UUT on which a DHCP-initiated IP subscriber session is configured.

  Conditions: The symptom is observed when the server is configured with a “Subscriber IP Address Assignment Using DHCP” based ISG session. When the client requests an IP address by sending the subscription request, it fails to negotiate a valid address from the DHCP pool configured on the server.

  Workaround: There is no workaround.

- CSCsx57711

  Symptoms: On a router configured with BGP VPNs, VRF removal may not work properly. VRF can remain in delete-pending state or BGP may crash at a later time.

  Conditions: The symptom is observed when the router is configured with one or more VRFs and has the BGP VPN address family enabled. The problem may be triggered by the deletion of a VRF from the router configuration through the **no ip vrf** or the **no vrf definition** commands. The issue is a race condition in the BGP code that deals with VRF net deletion and cleanup. Hitting the issue becomes more likely in large scale setups in terms of the number of configured VRFs and the number of nets in the BGP VPN table.

  Workaround: Make sure that all the nets in the BGP VPN table belonging to the VRF are deleted before issuing the VRF deletion command. To delete all the nets belonging to the VRF:

  1. All BGP CE neighbor configuration for that VRF must be removed.
  2. Any redistribution of routes into BGP for that VRF must be deconfigured.
  3. The import route-targets for the VRF must be removed.

Following the removal of the configuration, at least two minutes must elapse so that BGP can complete its cleanup. When no nets belonging to the VRF remain in the BGP table it should be safe to delete the VRF without the possibility of hitting this issue.

- CSCsx65705

  Symptoms: The router crashes upon executing the **no route-map** command with a match statement referencing an already-removed access-list.

  Conditions: The symptom is observed when the access-list is not present while executing the **no route-map** command.

  Workaround: Remove the match statements which are pointing to the access-list before the access-list is removed.

- CSCsx69555

  Symptoms: Unknown prefixes show up in the BGP table when “route-map” is configured on a neighbor and labels are sent from the other side.

  Conditions: The symptom is observed when the command **set mpls-label** is not given inside the route-map.

  Workaround: Give the command **set mpls-label** under all the route-maps configured on the neighbors.

- CSCsx70085

  Symptoms: Router watch failed.

  Conditions: Issue occurs randomly with a very low probability if you are running an HA system.

  Workaround: There is no workaround.

- CSCsx87562

  Symptoms: The following error is seen following interface range configuration change:

  ```
  %SYS-3-TIMERNEG: Cannot start timer (0xXXXXXXXX) with negative offset (- YYYYYYYYYY).
  -Process= "<interrupt level>", ipl= 2
  ```

  Conditions: This symptom is seen with dual supervisors installed and affects these Cisco Catalyst 4000 releases: 12.2(52)SG/XO, 12.2(50)SG4/5/6, 12.2(53)SG/SG1.

  Workaround:

  1. Configure the interfaces one by one.
  2. Force a switchover “redundancy force-switchover”.
  3. Use Cisco IOS Release 12.2(50)SG3 until the fix code is released.

- CSCsy08048

  Symptoms: Memory usage increases by about 10MB in processor memory following the creation of new checkpointing buffer pools. The result is less free memory available for other purposes.

  Conditions: This increase is of a fixed size, is seen immediately after boot, and is not configuration-dependent.

  Workaround: This issue should not impact most customers unless they are reaching the very limits of free memory with their configuration, in which case a reduction in the scale of configuration would work around the problem but may result in diminished features or scalability.

- CSCsy09743

  Symptoms: Multilinks flap after being added to an MLP bundle with a service policy attached to the interface.

Conditions: The symptom is observed when an existing service policy is on a interface. The interface is added to an MLP bundle without manually removing the service policy.

Workaround 1: Before adding the interface to the MLP bundle, remove the existing service policy configuration with the **no service-policy** command.

Workaround 2: If the link is already flapping, remove the MLP configuration with the **no ppp multilink** command then reapply the same service policy and remove it:

```
service-policy XXXXXXXXX
no service policy XXXXXXXX
```

Check that the queuing has been removed with **show hqf interface XXXX**. The command should return no output if the queuing has been removed. Add back the MLP configuration:

```
ppp multilink
ppp multilink group YYY etc
```

Workaround 3: Remove the channel-group and re-add it, if the interface was created as part of a channel-group.

Workaround 4: Use the **wr mem** command and reload the router.

- CSCsy24691

  Symptoms: For 6KW DC PS, some or all of the four power-input sensors are missing from SNMP entries in entPhyiscalTable “power-supply [1-2] power-input [1-4] Sensor”.

  Conditions: The symptom is observed with a 6KW DC Power Supply 2.

  Workaround: There is no workaround.

- CSCsy31601

  Symptoms: After switchover on UUT, BGP sessions will not be re-established and the RTRA will not accept a connection from the UUT.

  Conditions: The symptom is observed only if “timer 0 0” (hold-down timer never expires) is configured on DUT (where switchover is done) and there are no route changes on the RTRA. If any route is advertised or withdrawn by RTRA, the peer will send a TCP reset.

  Workaround: Do not use “timer 0 0” (hold-down timer never expires).

  Further Problem Description: This is observed in internal testing and is a rare case scenario.

- CSCsy34533

  Symptoms: Fast switching does not work when “dot1q native vlan” is configured on the interface.

  Conditions: The issue is seen with a Cisco 7600 series router.

  Workaround: Remove CLNS fast switching from the interface where the VLAN is configured.

- CSCsy34805

  Symptoms: Police rate configuration is lost after reload.

  Conditions: The following configuration:

  ```
  police rate 40000000 burst 1250000 peak-rate 60000000 peak-burst 1875000
  ```

  is saved in the router configuration as:

  ```
  police rate 40000000 bps burst 1250000 peak-rate 60000000 peak-burst 1875000
  ```

  This configuration is invalid and is rejected.

  Workaround: Configure using bytes per second and bytes as qualifiers:

  ```
  police rate 40000000 bps burst 1250000 bytes peak-rate 60000000 bps peak-burst 1875000
  bytes
  ```

- CSCsz11384

  Symptoms: The following error is logged:

  %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!)

  Conditions: Symptom observed in Cisco IOS Release 12.2(33)SRC in Cisco Intelligent Services Gateway (ISG) solution and with a very high rate of DHCP discoveries.

  Workaround: There is no workaround.

- CSCsz16961

  Symptoms: The system crashes when one of the 6PE multipath interfaces is shut down. All cards crash with the same decodes.

  Conditions: The symptom is observed with IPv6 Provider Edge (Cisco 6PE) router over MPLS with multiple paths.

  Workaround: There is no workaround.

- CSCsz24554

  Symptoms: The standby router reloads continuously.

  Conditions: The symptom is observed in highly scaled environments when the checkpointing facility may get permanently stuck to FLOW_OFF if the standby unit reloads when FLOW_OFF is asserted.

  Workaround: Reload the standby unit after executing the **test checkpoint flow on** command.

  Further Problem Description: Execute the **show checkpoint stat** command at the active router console CLI to determine if the flow control state is set to OFF.

- CSCsz25451

  Symptoms: The TX CPU crashes when there is a setup of 1K DMLP interfaces and when the SPAs are reloaded.

  Conditions: The symptom is observed in a highly-scaled configuration when the SPAs are reloaded.

  Workaround: There is no workaround.

- CSCsz40677

  Symptoms: PRE crash caused by DHCP internal function.

  Conditions: The symptom is observed when the router is running as a DHCP server.

  Workaround: There is no workaround.

- CSCsz66064

  Symptoms: VPLS FRR cutover takes much longer than expected (5-6 seconds), when the primary is on ES40 and backup on ES20.

  Conditions: The symptom is observed when VPLS VCs are going on the TE FRR tunnel, and cutover happens with the backup interface on ES20. The issue is seen with scaled VCs.

  Workaround: There is no workaround.

- CSCsz68709

  Symptoms: A console may lock when using the **scripting tcl init** *init-url* command.

  Conditions: This symptom is observed when using the **scripting tcl init** *init-url* command where the *init- url* is invalid or inaccessible, then entering the **tclsh** command and appending a file name.

  Workaround: Ensure that the *init-url* argument used in the **scripting tcl init** command is valid and accessible.

Alternate workaround: Enter the **tclquit** command to end the Tcl shell and return to privileged EXEC mode, then enter the **tclsh** command to enable the Tcl shell again.

- 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.

- 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.

- CSCsz81158

  Symptoms: Stale prefixes are seen in BGP tables because of missing withdrawals.

  Conditions: The symptom is seen in a scale setup where the UUT has hundreds of peers. After several hundred thousand prefixes have been exchanged, the removal of some prefixes at a neighbor will not cause the UUT to send withdrawals of those prefixes to the neighbors it has already advertised those prefixes to.

  Workaround: Do a hard reset.

- CSCsz83570

  Symptoms: SSH sessions disconnect during large data exchanges, such as large logs with pagers.

  Conditions: The symptom is observed when large amounts of data are exchanged between both ends: client and server (i.e.: the client provides a large input to the server and the server has a large output to send to the client). The session gets hung momentarily and disconnects after the timeout period of 120 seconds.

  Workaround: Use 3DES for encryption.

- CSCta06451

  Symptoms: Memory leak is observed in export packets when both OER and Netflow are enabled.

  Conditions: The symptom is observed only when both Netflow and OER export is enabled. OER export is enabled by default to a 3949 port.

  Workaround: There is no workaround.

- CSCta07104

  Symptoms: The **mpls bgp forwarding** command is not synced to the standby router.

  Conditions: When the **mpls bgp forwarding** command is not configured manually on the ASBR router, when eBGP Inter-AS session comes up, the command is auto-generated on the interface. The command is not synced to the standby router.

  Workaround: The issue will not be seen:

  1. When the **mpls bgp forwarding** command is configured manually.
  2. When the command is not configured manually, after a switchover, both the active router and the standby router will get that command.

- CSCta08194

  Symptoms: A router may crash.

  Conditions: This symptom is observed when reprovisioning an AToM tunnel with AAL5 encapsulation.

  Workaround: There is no workaround.

  Further Problem Description: A complex sequence of events with specific timing characteristics is required to hit this crash.

- CSCta08772

  Symptoms: EzVPN clients are failing negotiation. This may cause the router to use the less-specific route.

  Conditions: The problem can occur when 0/0 is configured as a destination and EXACT_MATCH is specified.

  Workaround: There is no workaround.

- CSCta20946

  Symptoms: ES+ line card crashes.

  Conditions: The symptom is observed with a port-channel with ethernet service instances. QoS is applied on both EVC and service group. Repeated rapid configuration and unconfiguration, involving removal of policy-maps and service groups.

  Workaround: There is no workaround.

  Further Problem Description: There are few conditions where improper clean up happens in platform QoS data structures leading to out of bound memory accesses. Memory corruption occurs, resulting in a crash with various signatures.

- CSCta31247

  Symptoms: On scaled SVI QoS (with a minimum of 100 SVIs), modifying the policy-map causes the ES+ line card to crash. The policy-map contains seven class-maps and actions.

  Conditions: The symptom is observed on a Cisco 7600 series router with an ES+ line card. A policy-map with multiple class-maps is configured and attached to 100 SVI (minimum) interfaces. The policy-map is modified dynamically. Additionally, overwriting the running configuration without any changes causes the line card crash.

  Workaround: There is no workaround.

- CSCta41186

  Symptom: QoS classification in SIP-400 LC does not work as expected when there are “deny” or “match not” entries.

  Conditions: There should be more than one deny entry (“match not” in class map or “deny” in ACL).

  Workaround: There is no workaround.

- CSCta43577

  Symptoms: ES20/6704/SIP400 line cards crash during bootup.

  Conditions: The symptom is observed when there are many line cards in the setup.

  Workaround: There is no workaround.

- CSCta45976

  Symptoms: A BFD session cannot be established to the peer if the same IP address is configured on the device in a different VRF.

  Conditions: The symptom is observed when BFD sessions stay in a down state.

  Workaround: Remove the locally-configured IP address.

- CSCta46107

  Symptoms: FTP transfers from FTP servers on internet to router fail, with “Connection timed out” or protocol errors.

  Conditions: The symptom is observed with the following conditions:

- Cisco 877, Cisco 1801, Cisco 1841 routers.
- Cisco IOS Release 12.4(24)T and 12.4(24)T1.

Workaround: There is no workaround.

Further Problem Description: Using TFTP or SCP works fine.

- CSCta46483

  Symptoms: The standby crashes upon deleting the “ip subscriber routed” configuration from the port-channel interface.

  Conditions: The symptom is observed upon the creation of a port-channel subinterface for a non-existing main interface. It is seen on deleting the configuration “ip subscriber routed” from the main interface. The standby crashes due to parser sync error (due to the configuration mismatch).

  Workaround: There is no workaround.

- CSCta49840

  Symptoms: GGSN may encounter a fatal error in VPDN/L2TP configurations.

  Conditions: The symptom is observed in rare race conditions when physical connectivity on the interface to LNS is lost while there are active sessions and traffic.

  Workaround: There is no workaround.

- CSCta56431

  Symptoms: L3VPN/6VPE traffic stops following an SSO when label mode is “per-vrf”.

  Conditions: The symptom is seen only when the label mode is changed from per-prefix configured initially. (If it is from the startup configuration, the issue is not seen.)

  Workaround: Perform a shut/no shut of the VRF interface.

- CSCta57455

  Symptoms: Cisco 7600 router processor may crash.

  Conditions: Occurs when a large packet to be multicast is replicated in the router in software switching path, and there are multiple such packets being processed in quick succession.

  Workaround: There is no workaround.

- CSCta61293

  Symptoms: When a port-channel with an EVC bridge-domain is undergoing a state transition, the Mroute table on the RP does not populate the SVI interface in the outgoing list. This SVI corresponds to the bridge-domain number specified in the EVC.

  Conditions: The symptom is observed with a port-channel EVC bridge-domain. When you perform a shut/no shut this issue is seen.

  Workaround: Remove then add “ip igmp join-group <>” under the SVI interface on the receiver router.

- CSCta71873

  Symptoms: Multicast traffic may not forward correctly to OIFs (which are port-channel/SVI) if there is a continuous link flap.

  Conditions: The symptom is observed when the OIF is a port-channel/SVI.

  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.

- CSCta75687

  Symptoms: BGP sends the withdrawn message to a peer as if a prefix was labeled (even though the prefix is not labeled). This can cause interoperability problems if the peer does not understand the message and may lead to routing loops in the network.

  Conditions: The symptom is observed on a router configured with BGP peering with another vendor’s router.

  Workaround: Unconfigure the send-label knob. (The existing session will flap since capability will have to be renegotiated.)

- CSCta77678

  Symptoms: RTP timestamp on the RFC 2833 event is modified. IP Phones are using RFC2833 to transport the DTMF signals, which causes problems with the Voicemail systems.

  Conditions: This symptom occurs when RTP header compression is enabled.

  Workaround: There is no workaround.

  Further Problem Description: The problem disappears if cRTP is disabled. The issue is seen with Class-Based cRTP configured and also with other cRTP configuration types.

- CSCta79313

  Symptoms: When the router is running EIGRP, there are a lot (hundreds) of routes in the routing table and when changes to the prefix-list are applied (it does not matter if it is currently used by EIGRP or not) high CPU is observed. The process that is causing high CPU is EIGRP-IPv4. Sometimes there can be observed a %SYS-3-CPUHOG for EIGRP-IPv4 process.

  Conditions: The issue is hardware independent so can be observed on any router with EIGRP prefix lists, and lots of routes in the RIB (routing table). Additionally there must be at least one redistribute command on EIGRP as well.

  Please note that problem could also occur without the BGP routing process, but the necessary condition is for the device to have many routes in the RIB table (BGP has been the logical source for introducing large numbers of routes to the routing table).

  Workaround: There is no workaround.

  Further Problem Description: To mitigate the impact of this issue, minimize changes to prefix lists or do during a scheduled maintenance window where brief periods of high CPU may not cause customer impact.

- CSCta85026

  Symptoms: CLI does not accept white spaces in the DHCP option 60 Vendor Class Identifier (VCI) ASCII string, and shows the following error message:

```
Router(dhcp-config)#option 60 ascii Cisco AP c1240

% Invalid input detected at '^' marker.

Router(dhcp-config)#
```

Conditions: The symptom is observed with Cisco IOS Release 12.4(24)T1 and later.

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.

- CSCtb04035

  Symptoms: Core dump capture is only allowed on bootflash/bootdisk of SP and not external disks, such as disk0: and disk1.

  Conditions: The symptom is observed when capturing core dump for debugging when there is not enough space left in SP bootflash.

  Workaround: There is no workaround.

  Further Problem Description: SP core dump can be written to bootflash/disk0:/disk1 using the command **exception** and the new argument *switch*.

- 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.

- CSCtb13846

  Symptoms: Standby resets upon changing the bandwidth of the policy attached to the MFR interface when in shut state.

  Conditions: The symptom is observed when you configure a policy-map to have a small bandwidth. Attach this service-policy onto the MFR interface which is in UP state. Next, shut down the MFR interface and modify the policy to take more bandwidth in the service-policy. The standby then resets.

  Workaround: Configure less bandwidth in the service-policy.

- CSCtb15699

  Symptoms: When accounting is enabled in both a TC prepaid service profile and the prepaid configuration, the prepaid accounting records are not sent.

Conditions: The symptom is observed when a TC service is applied to a PPP or IP session. Service profile has prepaid and accounting enabled. Prepaid configuration also has accounting enabled.

Workaround: There is no workaround.

- CSCtb17388

  Symptoms: Following a router reload, the following error message is seen:

  ```
  cmfi_vpnid_is_valid Invalid Vpn Id
  ```

  Conditions: The symptom is observed while reloading the router which has a large number of VRFs with IPv6 address-family, but no “ipv6 unicast-routing” enabled.

  Workaround: If not in “Host mode”, there is no need to have VRF IPv6 address-family without “ipv6 unicast-routing”. So simply remove VRF IPv6 address family or add “ipv6 unicast-routing”, save the configuration, and reload.

- CSCtb20650

  Symptoms: Occasionally, you may not be able to copy an image to the standby when the standby is in RPR mode. The following error is seen:

  ```
  TF I/O failed in data-in phase
  ```

  Conditions: The symptom is seen in RPR mode only.

  Workaround: Copy in SSO mode.

- CSCtb25549

  Symptoms: Router crashes.

  Conditions: The symptom is observed with the following sequence:

  1. Use the command **debug condition username**.
  2. Bring up a VPDN session.
  3. Clear the VPDN tunnel on LAC.
  4. Remove the conditional debug.

  Workaround: There is no workaround.

- CSCtb33899

  Symptoms: When CS5 packets are classified with DSCP-based WRED ES+ line cards, the packets should curve CS5 random drop counters, not the default. The random detect default drop counter is updated instead of CS5.

  Conditions: The symptom is observed with a DSCP-based WRED service policy applied in egress direction on an EVC local connect circuit on ES40 line card.

  Workaround: There is no workaround.

- CSCtb39430

  Symptoms: A malfunctioning line card or standby RP inserted into a running Cisco 7600 chassis can cause 99% packet loss for traffic entering CFC-based line cards.

  Conditions: The symptom is observed on any Cisco 7600 system with a malfunctioning line card/standby RP in a live system (logging SWITCH_BUS_IDLE error messages).

  Workaround: Power down line card by line card to identify the culprit line card/standby RP. Once the SWITCH_BUS_IDLE error messages stop it is likely the culprit has been identified.

  Further Problem Description: Flows between DFC cards are not affected.

- CSCtb41458

  Symptoms: IPv6 multicast traffic is process-switched on IPv6 RBE.

  Conditions: IPv6 Cisco Express Forwarding (CEF) is enabled, however IPv6 multicast traffic is process-switched on IPv6 RBE interface.

  Workaround: There is no workaround.

- CSCtb44299

  Symptoms: In certain situations, the standby reloads.

  Conditions: The problem occurs when the first CR is typed on the standby console at exactly the same time as a configuration command is executed on the active. The next command on the standby will cause the standby to reload.

  Workaround: Do not enable the standby console, or ensure that you are not configuring the active when the standby console is first used.

- CSCtb60261

  Symptoms: After defaulting the port-channel interface that has EVCs (with QoS) on them which are in turn members of service group with QoS on it, QoS resources in the line card are not deleted. Because of this, when EVCs with QoS are reconfigured on the port-channel interface the following error is seen:

  ```
  %X40G_QOS-DFC2-3-ACTN: Traffic Manager programming error. creation failed
  ```

  Conditions: This is more pronounced in a scale scenario. It only occurs with PC EVC. But can be observed with single EVC on a port-channel also. This is observed with an ES+ card.

  Workaround: Do not default/delete the port-channel interface when it has EVCs with QoS. Remove QoS on the EVC before deleting the EVC itself or before deleting the interface. That is, do not use the following commands before EVCs are removed on port-channel:

  default interface port-channel <>

  no interface port-channel <>

- CSCtb70344

  Symptoms: SCP messages are dropped by line cards. No response is sent to the NMP.

  Conditions: The symptom is observed when large numbers of continuous SCP messages are sent to a single line card.

  Workaround: Possibly pause SCP transmission to the line card and then retry.

  Further Problem Description: This mostly affects offline diagnostics as offline tests can send continuous SCP messages to the line card.

- CSCtb70578

  Symptoms: With L2PT and SPAN configurations in the same router, the following error message might be displayed on a Cisco 7609 router:

  ```
  %SPANTREE-SP-2-RECV_PVID_ERR: Received BPDU with inconsistent peer vlan id 1 on
   GigabitEthernet1/2 VLAN5.
   %SPANTREE-SP-2-BLOCK_PVID_LOCAL: Blocking GigabitEthernet1/2 on MST0.
   Inconsistent local vlan.
  ```

  Conditions: The symptom is observed under the following conditions:

  1. RSPAN is configured on the Cisco 7609 router.

2. STP BPDUs are being tunneled up to the Cisco 7609 router via L2PT.
3. L2PT is configured locally on the Cisco 7609 router.

Workaround: Apply a VACL where the RSPAN session is sourced:

```
mac access-list extended block_l2tp_dmac
 deny   any host 0100.0ccd.cdd0   L2PT destination mac
 permit any any

 vlan access-map block_l2tp 10
 match mac address block_l2tp_dmac
 action forward

vlan filter block_l2tp vlan-list 5   insert rspan vlan.  (In this case, it is 5)
```

- CSCtb70584

  Symptoms: With MSToEVC and N-PE redundancy enabled between two Cisco 7600 series routers in a ring topology, the assigned root Cisco 7600 series router blocks its connection to the other router due to a dispute state.

  Conditions: This issue is seen in a ring topology with MSToEVC and N-PE redundancy between two nodes. It occurs when there are valid active and backup MPLS-TE tunnels between the nodes. BPDUs travel across both tunnels (even though they should only traverse the primary) and cause the dispute state.

  Workaround: Disable the backup tunnel between the nodes, although this removes the redundancy in case the link between the nodes fails.

- CSCtb78266

  Symptoms: An incorrect NAS port ID is given when testing IDBless VLAN for PPPoE.

  Conditions: The symptom occurs on a Cisco 7200 router that is running Cisco IOS Release 12.4(15)T10.

  Workaround: There is no workaround.

- CSCtb79113

  Symptoms: If there is a PWE between two Cisco 7600 series routers and if one of the routers reloads, the PWE3 comes up once the device has booted after the reload but it does not pass any traffic.

  Conditions: The symptom is observed if there is a PWE between two Cisco 7600 series routers and if one of the routers is booted after a reload.

  Workaround: Take the xconnect statements off and apply them back on (sometimes on one side and sometimes both sides).

- CSCtb80410

  Symptoms: SP crash due to delay in the Standby Supervisor powering down during CBUS recovery.

  Conditions: The symptom is observed when the Standby Supervisor has a faulty backplane connector to jam the constellation bus.

  Workaround: There is no workaround.

- CSCtb81445

  Symptoms: A policy-map with “trust dscp” configured under a class-map is not accepted on a port-channel interface in ingress for LAN card member-links.

  Conditions: The symptom is observed on a Cisco 7600 series router. It is seen when a policy-map is configured with “trust dscp” under a class map and when this is attached to the port-channel interface in an ingress direction for the LAN card member-links on it.

  Workaround: There is no workaround.

- CSCtb86520

  Symptoms: Serial interfaces configured as Multilink Frame Relay (MRF) member links on SONET APS Protect line card may erroneously be in UP/UP state (they should be UP/DOWN) thereby resulting in the parent MFR interface being UP/UP, further resulting in dual connected routing entries in RIB. This causes a service outage as IP flows are forwarded to an APS PROTECT link and lost.

  Conditions: The symptom is observed under the following conditions:

  1. A Cisco 7600 series router with two WS-SUP720-3B cards and two OSM-1CHOC12/T1-SI.
  2. The router is running Cisco IOS Release 12.2(33)SRB5.
  3. Issue may occur during hard reset (removing the power) of the Cisco 7600 series router.
  4. Issue is reproducible by enabling member links on Protect MLFR line card first, then enabling member links on the active MLFR line card like this:

     A. Make sure all serial interface are in “shutdown” state.

     B. Configure two MFR bundles (say MFR1 and MFR2) and subinterfaces MFR1.1 and MFR2.1

     C. Configure four serial interfaces as a member of MFR1 under the OSM-1CHOC12/T1-SI which is in an inactive state.

     D. Configure another four serial interfaces as a member of MFR2 under the OSM-1CHOC12/T1-SI which is in SONET APS active state.

     E. Give “no shut” on the MFR serial member interfaces belonging to SONET APS inactive OSM-1CHOC12/T1-SI F. Give “no shut” on the MFR serial member interfaces belonging to SONET APS active OSM-1CHOC12/T1-SI

     Observe that all the MFR serial member interfaces configured are in “UP/UP” state and both (inactive and active OSM-1CHOC12/T1-SIs) MFR interfaces are also UP.
  5. Issue does NOT happen under same conditions when using MLPPP or straight serial links. 6. Issue also reproducible after simple reload in ~40% of reloads.

  Workaround 1: Perform a **shut**, **no shut** on APS Protect MFR interface.

  Workaround 2: Perform a **shut** on the member links configured under the inactive controller.

- CSCtb88060

  Symptoms: When unidirectional Ethernet (UDE) is configured, UDLD configurations are nullified. On taking out UDE configs, the port should re-participate in UDLD. But is not happening here.

  Conditions: The problem is seen if we configure **udld port aggressive** command.

  Workaround: To use the global command **udld enable**.

- CSCtb89424

  Symptoms: In rare instances, a Cisco router may crash while using IP SLA udp probes configured using SNMP and display an error message similar to the following:

```
hh:mm:ss Date: Address Error (load or instruction fetch) exception, CPU signal 10, PC
= 0x424ECCE4
```

Conditions: This symptom is observed while using IP SLA.

Workaround: There is no workaround.

- CSCtb90653

  Symptoms: TCP ports 4509, 4510, and 2222 are opened without any configuration.

  Conditions: The following releases are affected: Cisco IOS Release 12.2(33)SRD, 12.2(33)SRD1, 12.2(33)SRD2, 12.2(33)SRD2a, and 12.2(33)ZZ.

  Workaround: Disable the listening of the ports with the privileged CLI command: **test platform ezdriver deactivate**.

- CSCtb99472

  Symptoms: Doing an OIR of a PA-2CT3 Port Adapter in subrate mode causes some of the interface configurations to get lost and the subrate channels to go down.

  Conditions: The symptom is observed with Cisco 7200 series routers that is running with Cisco IOS Release 12.2(33)SRD2.

  Workaround: To reapply the serial configuration, perform a “shut/no shut”.

- CSCtc01196

  Symptoms: ISIS topology is broken after two or three consecutive SSOs with “isis nsf ietf” enabled. This causes routes to be missing in the routing table and permanent traffic loss.

  Conditions: The symptom is observed when “isis nsf ietf” is enabled and the restarting router comes up too slowly, causing neighboring routers on LAN interfaces to time out.

  Workaround: Perform a shut/no shut on the interface and ISIS will re-establish adjacency with the neighbors on the LAN interface.

- CSCtc04459

  Symptoms: High CPU is observed when sequential IMSI values are sent in a PDP request and, as a result, low NDR is observed.

  Conditions: The symptom is observed under the following conditions:

  1. GTP-SLB is configured.
  2. Sequential IMSI values are sent in a GTP PDP request.

  Workaround: Use random IMSI values.

- CSCtc15394

  Symptoms: The parity errors are seen on a 4XOC3-ATM 1XOC3-ATM 1XOC12-ATM SPA while it is operational and plugged into SIP200 or SIP400 chassis with or without traffic running.

  Conditions: No known conditions. Soft errors can happen any time due to environmental effects.

  Workaround: There is no workaround.

- CSCtc17058

  Symptoms: VC stops sending traffic due to duplicate VPN ID in port-based EoMPLS.

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

  Workaround: Do a shut/no shut on the interface (either on the same interface on which the VC has stopped sending traffic or an interface which has the port-based EoMPLS configured on the router).

- CSCtc17311

  Symptoms: TCAM device has corrupted data for valid entries seen in an X40G line card.

  Conditions: The symptom occurs during a background TCAM consistency checker.

  Workaround: There is no workaround.

  Further Problem Description: Ignore these messages as the entries are already corrected.

- CSCtc17429

  Symptoms: Multicast packets for some IP multicast groups get duplicated.

  Conditions: The symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRD2a and having an SRP ring as the OIF interface for IP multicast. The duplicate packets for those groups can be seen using the command **show ip mroute count** on the other nodes in the SRP ring.

  Workaround: There is no workaround.

- CSCtc22745

  Symptoms: Without PMTU configured and the interface MTU is 1500 on the L2TPv3 uplinks, packets are not fragmented.

  Conditions: Occurs with packets that require fragmentation between the L2TPv3 endpoints.

  Workaround: There is no workaround.

- CSCtc24864

  Symptoms: CDP is disabled and its neighbors are not seen on a CDP-enabled QnQ port after a shut/no shut operation.

  Conditions: The symptom is observed on an L2 QnQ tunnel port. By default, on L2 QnQ tunnel port CDP is disabled. CDP can, however, be enabled on a QnQ port through the command **cdp enable**. After enabling the CDP on a QnQ port, a subsequent link down and link up (shut and no shut) of this QnQ port results in disabling the CDP which is the default behavior.

  Workaround: Configure CDP (using the **cdp enable** command) again after link up.

- CSCtc24959

  Symptoms: Occasionally you may experience a multicast traffic loss in dual path line cards.

  Conditions: The symptom is observed in dual path line cards. Occasionally, met2 programming will go out of sync between two data paths.

  Workaround: Any change that triggers reprogramming that entry will help. Changing replication mode to ingress is a workaround.

- CSCtc32238

  Symptoms: mVPN traffic is not getting forwarded after SUP failover.

  Conditions: The symptom is observed under the following conditions:

  - The multicast traffic is flowing from ingress PE towards egress PE.
  - Used redundancy force-switchover or primary SUP OIR for the SUP failover on ingress PE.
  - Some of the mVPN traffic flows stopped forwarding the traffic.

  Workaround: There is no workaround.

- CSCtc33158

  Symptoms: A router may experience packet drops for the following packet byte size ranges, only when L2TPv3 cookies are enabled:

238-241

494-497

750-753

1006-1009

1262-1265

The following error will be reported when the packets are dropped:

```
%DEV_SELENE-DFC3-3-XAUI_LEN: Selene 0 XAUI 0 Packet Length Error
```

Conditions: The symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRD2, using an interface on a 7600-ES+40G3CXL module for a core-facing L2TPv3 tunnel.

Workaround: Disable L2TPv3 cookies.

- CSCtc36588

  Symptoms: After reload in Cisco IOS Release 12.2(33)SRD3, the MAC address of a port-channel, including member links on the supervisor, is set to 0000.0000.0000.

  Conditions: This issue is seen after a reload in Cisco IOS Release 12.2(33)SRD3 and when a port-channel has member links on the supervisor.

  Workaround: Configure the MAC address as follows:

  ```
  7600(config)#interface port-channel XY
   7600(config-if)#mac-address XXXX.YYYY.ZZZZ
  ```

- CSCtc37147

  Symptoms: RPF check fails when default route originates from IS-IS and the egress interface is a TE tunnel.

  Conditions: This symptom is observed when IS-IS is configured as the routing protocol and the default route originates from IS-IS.

  Workaround: Use the **ip mroute** command or route-leaking to set a specific route in the table. Enter **show ip route 0.0.0.0** to determine if the next hop for the default route is an MPLS tunnel interface. If it is, enter **ip mroute** to configure the real interface that the MPLS TE tunnel uses for the default route multicast nexthop.

  Alternate workaround: Use the OSPF routing protocol rather than IS-IS.

- CSCtc38796

  Symptoms: In some instances, when the Cisco 7600/RSP720/RP crashed and the core dump is configured to be created. But this coredump is corrupted and recognized by gdb.

  Conditions: This symptom is seen only with RSP720.

  Workaround: There is no workaround.

- CSCtc40677

  Symptoms: The distribute-list applied to the virtual-template interface is not effective for the virtual-access interfaces spawned by that template. For example, configured on the ASR (hub) is:

  ```
  router eigrp 1
    redistribute static metric 10000 100 255 1 1500
    network 10.0.0.0
    no auto-summary
  ```

```
  distribute-list prefix TEST out Virtual-Template1 !
ip route 0.0.0.0 0.0.0.0 Null0
!
ip prefix-list TEST seq 10 permit 0.0.0.0/0 ip prefix-list TEST seq 20 permit
10.0.0.0/8
```

and on the branch site connected via a virtual-access interface:

```
Branch#sh ip route eigrp
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%

      10.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
D       10.0.0.0/8 [90/46251776] via 10.12.0.2, 00:00:06, Dialer1
D       10.1.1.0/24 [90/46228736] via 10.12.0.2, 00:00:06, Dialer1
D       10.2.2.0/24 [90/46354176] via 10.12.0.2, 00:00:06, Dialer1
D*EX 0.0.0.0/0 [170/46251776] via 10.12.0.2, 00:00:06, Dialer1
```

This shows that no filtering was applied, since the 10.1.1.0/24 and 10.2.2.0/24 should have been dropped off the updates.

Conditions: The symptom is observed on a Cisco ASR 1000 series router that is running Cisco IOS Release 12.2(33)XND1.

Workaround: Configure the distribute-list for the specific virtual-access interface used for the connections on the hub.

- CSCtc41760

  Symptoms: A Cisco 6500 may experience redzone crash at UDLD process. The following message may appear:

  ```
  %SYS-SP-3-OVERRUN: Block overrun at 44456570 (red zone 6D000700)
  -Traceback= 40291448 402938DC 40D74570 40D763A0
  ```

  Traceback will vary from code to code.

  Conditions: UDLD is configured

  Workaround: Disable UDLD.

- CSCtc46171

  Symptoms: LTLs leak for VPLS VC after an SSO.

  Conditions: The symptom is observed with “Auto Discovery” VPLS VCs after an SSO.

  Workaround: There is no workaround.

- CSCtc46174

  Symptoms: A Cisco 10000 series router that is configured for ISG has no limit for number of redirected sessions which could result in high CPU.

  Conditions: This symptom is observed on a Cisco 10000 series router that is running ISG and Cisco IOS Release 12.2(33)SB or 12.2(31)SB.

  Workaround: There is no workaround.

- CSCtc46512

  Symptoms: There is a crash in SSR regression.

Conditions: The symptom is observed when a service policy is applied on a session and traffic is flowing through the session. This applies to IOU (simulator) images only.

Workaround: There is no workaround.

- CSCtc52149

  Symptoms: SIP200 CPU 1 crashes as indicated below.

  ```
  SLOT 4: Aug 16 14:42:52.115 KSA: %R4K_MP-3-CRASHED: CPU 1 has now crashed a total of
  1 times
  ```

  Conditions: There is no specific trigger to this problem. It happens randomly and recovers on its own.

  Workaround: There is no workaround.

- CSCtc52236

  Symptoms: SIP module crash.

  Conditions: There is no specific trigger to this problem. It happens randomly and recovers on its own.

  Workaround: There is no workaround.

  Further Problem Description: This happens when an IP packet removes padding calculated from ATM control.

- CSCtc52740

  Symptoms: Cisco 7600 ES+ interface will not accept policy map with “random-detect cos-based” statement.

  Conditions: CLI configuration is rejected on main interface of an ES+ line card.

  Workaround: There is no workaround.

- CSCtc57044

  Symptoms: The **mpls propagate-cos** command may not function correctly on a Cisco 7600 router.

  Conditions: This was observed on several Cisco 7600s running Cisco IOS Release 12.2(33)SRC.

  Workaround: Remove and reapply the **mpls propagate-cos** command.

- CSCtc58898

  Symptoms: In MPLS VPN scenario, if it happens that default route known via RIP in VRF is looping, route might stay in RIB.

  Conditions: Issue observed in Cisco IOS Release 12.2(33)SRC4 and 12.2(33)SRC5.

  Workaround: Clear VRF routing table of with the **clear ip route vrf** *name* ***** command.

- CSCtc60458

  Symptoms: On a Cisco 7600 router with a large number of VCs and VLANs, traffic stops forwarding traffic for several seconds while standby supervisor is booting.

  Conditions: Occurs on a router running Cisco IOS Release 12.2(33)SRC4.

  Workaround: There is no workaround.

- CSCtc60463

  Symptoms: The **traceroute mac** *src_mac dst_mac* command can cause a software crash on a Cisco 7600 router when configured with a large number of VLANs.

  Conditions: This occurs on a Cisco 7600 router running Cisco IOS Release 12.2(33)SRC4.

Workaround: Do not use the **traceroute mac** *src_mac dst_mac* command. Use a specific VLAN ID when using this command.

- CSCtc60958

  Symptoms: After the line card reset or router reload, the CLI (committed as part of CSCtb88169) does not get applied.

  Conditions: The issue is seen with a router reload or line card reset.

  Workaround: Reconfigure the command manually once the line card is up.

- CSCtc61025

  Symptoms: For VPLS autodiscovered pseudowires using FEC129, the label release message is not understood by the peer in Inter-op tests.

  Conditions: The symptom is observed when you delete the VFI or shut the attachment circuit to cause the label withdraw message to be sent. The peer will correspondingly send the label release message.

  Workaround: There is no workaround.

- CSCtc75774

  Symptoms: Protect channel shows signal failure with working channel even though working channel is up and working correctly.

  Conditions: The symptom is observed when the protect channel acts as an active controller and when you do a shut/no shut on the working channel which acts as an inactive controller.

  Workaround: There is no workaround.

- CSCtc77028

  Symptoms: A Cisco 10000 series router with a mix of passthrough, TAL, prepaid and postpaid sessions may experience a memory leak at sss_pm_post_authorization_cleanup.

  Conditions: The symptom is observed on a Cisco 10000 series router running a PRE-3 and Cisco IOS Release 12.2(33)SB7.

  Workaround: Reload the router.

- CSCtc81653

  Symptoms: The system crashes if the port-channel is removed while it is serving data traffic.

  Conditions: Port-channel is configured with the member links in it. The traffic is sent through the port-channel. If the port-channel is removed, the system sometimes crashes.

  Workaround: There is no workaround.

- 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.

- CSCtc87700

  Symptoms: A Cisco 7600 router may fail to process ingress Link Integrity Protocol messages on MFR serial link members, which will disallow Multilink Frame Relay interfaces from enabling.

  Conditions: This symptom occurs on a Cisco 7600 router with SUP-720-3BXL and OSM CHOC12, and running Cisco IOS Release 12.2(33)SRC and 12.2(33)SRD. This issue happens when MFR serial members are configured on CHOC12 OSM but may also occur on other line cards.

  Workaround: There is no workaround.

- CSCtc87822

  Symptoms: On a PE router, eBGP-learned VRF routes might not be advertised to eBGP neighbors in the same VRF.

  Conditions: The symptom is observed if DUT first learns the route from IBGP-VPNv4 (same RD) and then learns the route from the CE.

  Workaround: Soft clear towards the CEs missing the routes.

- CSCtc90579

  Symptoms: Router crashes due to memory corruption during MPLS TE auto backup tunnel deletion.

  Conditions: Caused by topology changes triggering backup tunnel deletion and RSVP hello mechanism.

  Workaround: Gloablly, disable RSVP hello and enable BFD hello:

```
Router(config)#no ip rsvp signalling hello
Router(config)#ip rsvp signalling hello bfd
Per MPLS TE enabled interface:
Router(config-if)#no ip rsvp signalling hello
Router(config-if)#ip rsvp signalling hello bfd
```

- CSCtc94339

  Symptoms: Multicast traffic is not forwarded in an egress direction via GRE over MPLS after a switchover.

  Conditions: The symptom is observed with GRE over MPLS with PIM enabled on the tunnel interface, from a Cisco 7600 series router in SSO redundancy mode.

  Workaround: Reload the router.

Further Problem Description: Identification of this issue can be seen when “dindex” shows as 0x0. In working state it is 0x7FFA:

```
show mls cef adjacency encap-tunnel detail
Index: 30      mtu: 1522, vlan: 1016, dindex: 0x0, l3rw_vld: 1 <<<<
               format: ENCAP-TUNNEL, flags: 0x11103500008600
               ip_sa: 10.10.10.10 ip_da: 10.20.20.20, tos: 0 ttl: 255
               wccp_hdr: 0, gre_hdr: 800
               packets: 415, bytes: 48970
```

- CSCtc94873

  Symptoms: After few show memory commands the telnet session to a Cisco 7600 series router is suspended and the router crashes. Traceback shows:

  ```
  -Traceback= 406AAEA0 406AB400 418164AC 418050B8 4067460C 406787E4 4067B7D8 4063076C
  423BB0F4 4065D058 417CB1C8 417CB1B4 Decode
  ```

  Conditions: The symptom is observed with a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRD3 and with “show memory” commands.

  Workaround: Do not use show memory fragment commands.

  Further Problem Description: When BFD is enabled and when the command **show memory [fast] fragment detail** is invoked, the crash/hang is observed at times. This is partially fixed with this DDTS to overcome SCHED-SEMNOTLOCKED error. Another part of it is fixed with CSCtd94438.

- CSCtd00054

  Symptoms: Link flap/down on PA-MC-T3E3-EC interface.

  Conditions: This symptom is observed when changing encapsulation after reload.

  Workaround: Perform an online insertion and removal (OIR) of the PA.

- CSCtd00479

  Symptoms: When ISIS is configured for NSF IETF, if the restarting router is a DIS on the LAN, after a switchover the ISIS database and topology could be incorrect. This results in an incorrect routing table.

  Conditions: The symptom is observed when ISIS is configured for NSF IETF and a switchover occurs.

  Workaround: Use NSF CISCO, or disable NSF.

- CSCtd15853

  Symptoms: When removing VRF configuration on remote PE, local PE receives withdraw message from remote PE to purge its MDT entry. However, local PE does not delete the MDT entry.

  ```
  /// Topology ///

                    iBGP
           <------------------->
     12.2(33)SB7              12.0(27)S4a
     1.1.1.1/32               2.2.2.2/32
     PE1(UUT)    ------------ PE2
  ```

  PE1 receives MDT entry from PE1 and PE2.

Please focus a entry of “2.2.2.2/32” from PE2.

```
PE-1
---
PE1-PRE2#
PE1-PRE2#sh ip bgp ipv4 mdt all
BGP table version is 13, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf V1)
*> 1.1.1.1/32       0.0.0.0                                0 ?
*>i2.2.2.2/32       2.2.2.2                  0    100      0 ? <<<---- HERE
*>i3.3.3.3/32       3.3.3.3                  0    100      0 ?
---
```

To trigger the issue, vrf configuration is remove on PE2.

You can see that PE2 sends withdraw message to PE1(1.1.1.1).

```
PE-2
---
PE2-PRE1#
PE2-PRE1#
PE2-PRE1#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
PE2-PRE1(config)#
PE2-PRE1(config)#no ip vrf V1
Tunnel interface was deleted. Partial configuration may reappear on reuse.
% IP addresses from all interfaces in VRF V1 have been removed
PE2-PRE1(config)#
PE2-PRE1(config)#
*Nov  9 12:29:35.447: %LINK-5-CHANGED: Interface Tunnel3, changed state to
administratively down
*Nov  9 12:29:36.467: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel3,
changed state to down
PE2-PRE1(config)#
PE2-PRE1(config)#end
PE2-PRE1#
PE2-PRE1#
*Nov  9 12:30:05.435: BGP(2): nettable_walker 2:1:1:2.2.2.2/32 no best path
*Nov  9 12:30:05.435: BGP(2): 1.1.1.1 send unreachable 2:1:1:2.2.2.2/32
*Nov  9 12:30:05.435: BGP(2): 1.1.1.1 send UPDATE 2:1:1:2.2.2.2/32 --
unreachable <<--- HERE
*Nov  9 12:30:05.435: BGP(2): updgrp 1 - 1.1.1.1 enqueued 1 updates,
average/maximum size (bytes) 45/45
PE2-PRE1#
```

```
PE2-PRE1#
PE2-PRE1#sh ip vrf

PE2-PRE1#
```

The MDT entry(2.2.2.2/32) is not deleted even if PE1 indeed receives withdraw message from PE2. “clear ip bgp *” would be needed to purge the MDT entry.

```
PE-1
---
PE1-PRE2#
*Nov  9 12:29:34.323: BGP:from:3 to:4 update format 1:1:3.3.3.3/0 MDT grp
239.0.0.1 pfxptr->masklen 96
*Nov  9 12:29:34.323: BGP:from:3 to:4 update format 1:1:1.1.1.1/0 MDT grp
239.0.0.1 pfxptr->masklen 96
*Nov  9 12:29:34.323: BGP(4): 2.2.2.2 send UPDATE (format) 2:1:1:1.1.1.1/32,
next 1.1.1.1, label 0, metric 0, path Local
*Nov  9 12:29:34.323: BGP:from:3 to:4 update format 1:1:2.2.2.2/0 MDT grp
239.0.0.1 pfxptr->masklen 96
*Nov  9 12:29:34.323: BGP(4): updgrp 1 - 2.2.2.2 updates replicated for neighbors:
*Nov  9 12:30:05.799: BGP(4): 2.2.2.2 rcv UPDATE about 1:1:2.2.2.2/64 --
withdrawn, label 3 <<--- HERE
*Nov  9 12:30:05.799: BGP: 2.2.2.2 Modifying prefix 1:1:2.2.2.2/64 from 4 -> 3
address
PE1-PRE2#
PE1-PRE2#sh ip bgp ipv4 mdt all
BGP table version is 13, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf V1)
*> 1.1.1.1/32       0.0.0.0                                0 ?
*>i2.2.2.2/32       2.2.2.2                  0    100      0 ? <<---- HERE
*>i3.3.3.3/32       3.3.3.3                  0    100      0 ?
PE1-PRE2#

PE1-PRE2#
PE1-PRE2#clear ip bgp *
PE1-PRE2#
*Nov  9 12:31:22.043: %BGP-5-ADJCHANGE: neighbor 2.2.2.2 Down User reset
*Nov  9 12:31:22.043: %BGP_SESSION-5-ADJCHANGE: neighbor 2.2.2.2 VPNv4 Unicast
topology base removed from session  User reset
*Nov  9 12:31:22.043: %BGP_SESSION-5-ADJCHANGE: neighbor 2.2.2.2 IPv4 MDT
topology base removed from session  User reset
```

```
*Nov  9 12:31:22.043: %BGP-5-ADJCHANGE: neighbor 3.3.3.3 Down User reset
*Nov  9 12:31:22.043: %BGP_SESSION-5-ADJCHANGE: neighbor 3.3.3.3 VPNv4 Unicast
topology base removed from session  User reset
*Nov  9 12:31:22.043: %BGP_SESSION-5-ADJCHANGE: neighbor 3.3.3.3 IPv4 MDT
topology base removed from session  User reset
*Nov  9 12:31:22.555: %BGP-5-ADJCHANGE: neighbor 3.3.3.3 Up
*Nov  9 12:31:22.563: BGP(3): 3.3.3.3 rcvd UPDATE w/ attr: nexthop 3.3.3.3,
origin ?, localpref 100, metric 0
*Nov  9 12:31:22.563: BGP(3): 3.3.3.3 rcvd 1:1:3.3.3.3/32
PE1-PRE2#
PE1-PRE2#
PE1-PRE2#sh ip bgp ipv4 mdt all
BGP table version is 1, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf V1)
* i3.3.3.3/32       3.3.3.3                  0    100      0 ?
---
```

Conditions:

- mVPN is configured on PE router.
- Both Pre-MDT SAFI and MDT-SAFI IOS are running in a Multicast Domain.

CCO : MDT SAFI

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/ps6604/ps6651/prod_white_paper0900aecd80581f3d.html

Workaround: There is no workaround.

- CSCtd21590

  Symptoms: RP crashed after executing **no import ipv4 unicast map filter**.

  Conditions: BGP import events debugging is on with **debug ip bgp import updates** or **debug ip bgp import event**.

  Workaround: Do not enable **debug ip bgp import event** or **debug ip bgp import update**.

- CSCtd25133

  Symptoms: Router gets into APS channel mismatch state.

  Conditions: Observed with MGX connected as APS peer, when both MGX cards (active and standby) are reloaded simultaneously.

  Workaround: Force APS switchover.

- CSCtd25933

  Symptoms: Active or standby RP crashes on executing the **shut** then **no shut** commands on the interface.

Conditions: The symptom is observed with the following conditions:

1. Encapsulation QnQ (or dot1q) is configured and removed on the sub-interface, on a WAN interface (SIP400).
2. Same VLAN configured as Encapsulation QnQ (or dot1q) on a LAN interface (ES+).
3. Perform shut/no shut on the ES+ interface.

Workaround: There is no workaround.

- CSCtd27247

  Symptoms: The router crashes when doing concurrent VRF add and deletion configurations.

  Conditions: The symptom is observed when a multiple configuration terminal is doing concurrent VRF add and deletion configurations.

  Workaround: Do not do concurrent VRF addition and deletion.

- CSCtd33145

  Symptoms: On a Cisco 10000 series router/PRE-3 that is running Cisco IOS Release 12.2(33)SB7 and ISG, the memory on the standby RP may become severely fragmented due to some SSS functions.

  After an SSO switchover, the new-active RP initially takes over with fragmented memory causing frequent malloc errors and eventually requiring a reload to recover.

  Conditions: The symptom is observed on a Cisco 10000 series router/PRE-3 that is running Cisco IOS Release 12.2(33)SB7 with 10K ISG sessions in a mix of web-login, TAL, prepaid, and passthrough.

  Workaround: A reload will recover memory.

- CSCtd35091

  Symptoms: The input queue on ISG access interface gets filled up causing the interface to wedge.

  Conditions: The symptom is observed when an L2-connected IP session for a client exists on the ISG and traffic from that client comes in with a different IP address to the one used to identify the session. This traffic is dropped and interface wedging is observed.

  Workaround: There is no workaround other than a router reload.

- CSCtd40804

  Symptoms: The EVC configuration does not exist on the ES20 line card. The first “show” command (below) shows that the EVC was known to the Route Processor (RP) on the Supervisor Engine, while the second command shows that the EVC did not exist on the ES20 line card in slot 4:

```
#sh ethernet service instance id 3555 interface gi4/0/1
Identifier Interface State CE-Vlans
3555 GigabitEthernet4/0/1 UP

#remote command mod 4 sh ethernet service instan id 3555 int gi4/0/1
EFP ID 3555 on interface GigabitEthernet4/0/1 does not exist
```

  Conditions: The symptom is observed after a Supervisor switchover.

Workaround: There are two workarounds for this issue. Both require that every port on the ES20 be configured prior to a switchover. If this is done, then the problem will not exist after a switchover and new EVCs can be successfully added following the switchover.

1. Configure at least one service instance under each interface on the ES20. An example is shown below:

```
interface GigabitEthernet1/0/3
    service instance 1 ethernet
    encapsulation dot1q 3
```

2. Configure "ethernet uni id *name* under each interface on the ES20. An example is shown below:

```
interface GigabitEthernet1/0/5
    ethernet uni id gi_1_0_5
```

- CSCtd54338

  Symptoms: The following output from the command **show ip rtp header-compression**, shows that one channelized serial interface has a large accumulated number of "seconds since line card sent last stats update" compared with another channelized serial interfaces in device with the same platform:

```
GR_SA_CORE_7613R_1#show ip rtp header-compression Serial1/2/0.1/3/1:0
RTP/UDP/IP header compression statistics:
  Interface Serial1/2/0.1/3/1:0 (compression on, Cisco)
  Distributed fast switched:
  10364 seconds since line card sent last stats update
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 16 rx slots, 16 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 0 free contexts
```

  Conditions: The symptom is observed with the following conditions:

  – Cisco IOS Release 12.2(33)SRD3.
  – Platform: Cisco 7613 router.
  – RP: RSP720-3CXL-GE.
  – SIP: Cisco 7600 SIP-200.
  – SPA: SPA-1XCHSTM1/OC3.

  This issue normally begins to show when the count of the channelized subinterface (number of cRTP sessions) is 200 or over.

  Workaround: Disable then enable RTP header-compression on the interface.

  Further Problem Description: The issue can be resolved by using **disable cRTP** and **enable cRTP** on each subinterface (see DDTS CSCso48621). However, sometimes the problem can reoccur in a few days after recovery on the same subinterface.

- 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.

- CSCtd66014

  Symptoms: ES+ line card crashes at powerup of a Cisco 7600 router that is running Cisco IOS 12.2SRE image if either the Traffic Manager or Frame memories in the ES+ Network processors report a double bit ECC error. The ES+ line card crashinfo will have the following string:

  ```
  %NP_DEV-DFC2-3-ECC_DOUBLE: Double-bit ECC error detected on NP 0, Mem 19, SubMem
  0x1,SingleErr 1, DoubleErr 1 Count 1 Total 1
  ```

  Conditions: Router reloads, OIR of ES+ cards, system environment temperatures that slowly vary around an ambient temperature of about 30 degreesC. This happens at system powerup. We have seen double bit ECC problems reported after a few hours of traffic if the ambient temperatures vary around 30 degreesC.

  Workaround: No configuration workaround is available. The line card will reset itself and will be operational in the second reload.

- CSCtd66918

  Symptoms: Standby Supervisor continually resets during detection of bad hardware in the system.

  Conditions: The symptom is observed when the bad line card is inserted in the slot following the Standby Supervisor slot (e.g.: Standby Supervisor in slot 6 and bad line card in slot 7).

  Workaround: There is no workaround.

- CSCtd72426

  Symptoms: Checkpointing facility on the standby SP is leaking memory buffers. This can lead to a WATERMARK error message.

  Conditions: The symptom is observed with the checkpointing facility on the standby SP.

  Workaround: There is no workaround.

  Further Problem Description: This issue can be checked with the command **show ipc session all verbose** from the standby SP. This output will show more messages requested then messages returned for the client “CHKPT:STANDBY SP” and this difference will grow every day. The **show check client** command from the standby SP will show the buffers held for “REP CHKPT CLIENT” and that this value is increasing over time.

- CSCtd72462

  Symptoms: A Cisco 7600 series router with an RSP720-3C processor may unexpectedly reboot after the **show policy-map interface** command is executed.

  Conditions: The issue is seen when there is a policy map on an interface with the following:

  - No set action.
  - No shared aggregate policer action.
  - No aggregate policer action.
  - uflow policer with “conform action” configured.

  Workaround: There is no workaround.

- 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

- CSCtd75248

  Symptoms: With QoS is disabled globally and when the ES20 interface is configured as a trunk, if traffic is sent with a valid COS value, the ES20 re-marks all COS values to “0”.

  Conditions: The symptom is observed when QoS is globally disabled.

  Workaround: Enable QoS globally using **mls qos** and trust the ES20 trunk interface to retain CoS values using **mls qos trust cos**.

  Further Problem Description: This issue is not seen in Cisco IOS Release 12.2(33)SRB. It is present in Cisco IOS Release 12.2(33)SRC onwards

- CSCtd77905

  Symptoms: Traffic will not flow properly for the first VRF, if there is a switchover from active to standby. This issue occurs because of a race condition.

  Conditions: The symptom is observed only in the HA setup.

  Workaround: Delete and reconfigure the problematic VRF.

  Further Problem Description: The problem is a timing issue. In the standby Supervisor, the aggregate labels are not getting programmed properly for the first VRF configured in the system.

- CSCtd83819

  Symptoms: Traffic drops on SIP400 upon unconfiguring and reconfiguring “bre-connect *vlan-id*”.

  Conditions: The symptom is observed when you unconfigure and reconfigure “bre-connect *vlan-id*”.

  Workaround: Remove and reconfigure the PVC, or reload the SPA, or do an APS switchover.

- CSCtd87264

  Symptoms: DHCP unicast BootP offers can not be propagated back in the incoming interface as the ARP entry is missing. This happens only when the relay function is combined in a VRF and the incoming interface is unnumbered.

  Conditions: The symptom is observed when SRD/SRE Cisco 7600 series router is a DHCP relay/snooping agent. The request must come in a VRF.

Workaround: Move the relay agent function to the global routing table.

- CSCtd90429

  Symptoms: VPLS traffic occasionally gets blackholed after multiple iterations of mid-point failure or reoptimization.

  Conditions: The symptom is observed when the core-facing interfaces are SIP400.

  Workaround: Perform a shut/no shut on the TE tunnel interface.

- CSCtd91012

  Symptoms: If BRE configurations are present on the HWIDB, when you configure an APS group an error message will be thrown to remove the BRE configurations.

  Conditions: The symptom is observed when there are BRE configurations on the HWIDB and you try to configure an APS group.

  Workaround: Remove the BRE configurations and then configure the APS group.

- CSCtd94128

  Symptoms: On ES+ cards, packets in the egress direction do not have the outer tag preserved.

  Conditions: This is seen on a port-mode configuration for an L2TPv3 tunnel where tagged packets are sent from the subscriber. The outer tag is always rewritten to null while the COS bits are preserved.

  Workaround: There is no workaround.

- CSCtd94438

  Symptoms: When the **show memory** *fast* **fragment detail** command is given, it leads to a crash of the Cisco 7600 series router. The console logs show some semaphore lock-related messages, IPC/XDR messages, and RP crash-related messages.

  Conditions: The symptom is observed when BFD is enabled and the **show memory** *fast* **fragment detail** command is given.

  Workaround: Avoid using the **show memory** *fast* **fragment detail** command, or disable BFD from the startup configuration and reload the router.

  Further Problem Description: If BFD is disabled in the startup configuration (i.e.: BFD is not configured when bringing up the router) the crash is not seen.

- CSCtd99244

  Symptoms: ES+ line card crashes reporting double bit ECC error.

  Conditions: This symptom occurs usually in the initial phases of line card bootup, but this has also been reported after a few hours of traffic through the ES+ line card ports.

  Workaround: There is no workaround. The ES+ may not report this error in the second reload. If errors persist, powercycle the chassis, or OIR the ES+.

- CSCtd99248

  Symptoms: There could be occasional double bit ECC errors for the traffic manager and other metadata memories that are reported on the Network processor on the ES+ line card.

  Conditions: This symptom is observed when the router reloads, OIR of ES+ cards, system environment temperatures that slowly vary around an ambient temperature of about 30 degreesC. This happens at system powerup. We have seen double bit ECC problems reported after a few hours of traffic if the ambient temperatures vary around 30 degreesC.

  Workaround: No configuration workaround is available. The line card will reset itself and will be operational in the second reload.

- CSCte14504

  Symptoms: Router crash with TLB (load or instruction fetch) exception.

  Conditions: The symptom is observed with a reload of the router that is running a Cisco IOS SRD Release.

  Workaround: There is no workaround.

  Further Problem Description: This is memory issue and so it might not be seen at every reload. In the local testbed, the crash is seen after a reload with a few VRF configurations under VLAN.

- CSCte21958

  Symptoms: A Cisco router may reload when an L2TP xconnect pseudowire is configured using a pseudowire class that has not yet been defined.

  Conditions: This symptom is observed when the following sequence of commands is entered:

  - `configure terminal`
  - `interface Ethernet0/0.1`
  - `encapsulation dot1Q 400`
  - `xconnect 10.0.0.1 555 encapsulation l2tpv3 pw-class test`
  - `pseudowire-class test`
  - `encapsulation l2tpv3`
  - `protocol l2tpv3 test`
  - `ip local interface Loopback0`
  - `vpdn enable`

  This symptom affects all platforms.

  Workaround: Define the pseudowire class using the **pseudowire- class** configuration command before referencing that pseudowire class in an xconnect configuration.

- CSCte28933

  Symptoms: L2TPv3 VLAN-mode reassembled packets get dropped on ES+.

  Conditions: The symptom is observed when “L2TPv3 cookie” is configured and L2TPv3 packets get fragmented in the core or at source.

  Workaround: Configure L2TPv3 without cookies.

- CSCte37192

  Symptoms: Traffic is dropped in the egress by SIP400.

  Conditions: The symptom is observed when BRE is configured, then removed, then reconfigured. Then perform a shut/no shut on the interface where the PVC is present.

  Workaround 1: Perform a shut/no shut on the interface.

  Workaround 2: Perform a SPA OIR.

- CSCte38652

  Symptoms: The standby reloads due to one of the line cards getting powered down with the reason given as: “Failed to configure the line card”.

  Conditions: The symptom is observed with a fully-loaded setup with all ESM20G cards and a large amount of configuration.

  Workaround: There is no workaround.

- CSCte38681

  Symptoms: Configuration sync error is seen upon enabling/disabling AAL5 encapsulation along with two reloads.

  Conditions: The symptom is observed only with a reload and upon disabling/enabling the AAL5 encapsulation.

  Workaround: Reload the router.

- CSCte46834

  Symptoms: The router crashes.

  Conditions: The symptom is observed with the following steps on the PE:

  ```
  config t
  ip vrf vpna
  import map IMPORT99 (this is the trigger).
  ```

  Workaround: There is no workaround.

- CSCte48935

  Symptoms: Following a reload, the ES20 port is unbundled from the port-channel and the following error message is shown:

  ```
  Port-channel10 and TenGigabitEthernet9/0/0 have different trust states
  ```

  Conditions: The symptom is observed with “mls qos” disabled globally and “mls qos trust” disabled on the ES20 interface.

  Workaround: Enable “mls qos” on the router. If “mls qos” is not desired, there is no workaround.

- CSCte50573

  Symptoms: Degraded performance with RLB and T-RLB.

  Conditions: The symptom is observed with the following conditions:

  1. SLB is configured with service radius.
  2. High CPU even at lower rates of 300 TPS.
  3. Cisco IOS Release 12.2(33)SRE.

  Workaround: There is no workaround.

- CSCte56594

  Symptoms: Seeing two dips of traffic drop after SSO, the first dip is about 80 milliseconds, the second traffic dip up to about 30 seconds.

  Conditions: This symptom is observed on the PE (Cisco 7609-S) that is configured with OSPF NSF and both MPLS and RSVP GR. Also 4K vlans, 20K virtual circuit is configured peering with another 5 PEs on the VPLS domain. Generate 60M unidirectional traffic across this VPLS domain, then execute redundancy switchover via CLI.

  Workaround: There is no workaround.

- CSCte58686

  Symptoms: Link flaps after an upgrade to Cisco IOS Release 12.2(33)SRD3.

  Conditions: The symptom is observed following an upgrade from Cisco IOS Release 12.2(33)SRB5 to SRD3.

  Workaround: There is no workaround.

- CSCte58749

  Symptoms: Some interfaces start flapping upon upgrading to Cisco IOS Release 12.2(33)SRD3.

  Conditions: This is a corner case condition. The interface flaps occur under following conditions:

  1. The peer connected on the other side of the interface sends a CODEREJ for a valid ECHOREP sent by a Cisco router.
  2. On receiving CODEREJ for ECHOREP, the router terminates the PPP session. The PPP sessions restart, and the interface flaps.

  Workaround: Disable keep-alive on the misbehaving peer router.

- CSCte67196

  Symptoms: On a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRD3 equipped with an OSM-CHOC12 line card, if a member link is removed and re-added to a multilink group during periods of congestion, the multilink interface may not recover its full transmit bandwidth.

  This issue only occurs when "service-policy output" is configured on the multilink interface and when this service policy contains queuing actions.

  This condition may be accompanied by the "show policy-map" interface failing to update packet counters and offered rate.

  Conditions: The symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRD3 equipped with an OSM-CHOC12 line card aggregating multilink interfaces using queuing policy-maps.

  Workaround: Remove and reapply "service-policy output" from the degraded multilink interface.

- CSCte68259

  Symptoms: Random end-to-end traffic failure with an ES+ line card with L2TPv3 termination on one port which is interfacing with EVC BD remotely.

  Conditions: This issue occurs when the ES+ line card is configured with the L2TPv3 feature.

  Workaround: There is no workaround.

- CSCte95228

  Symptoms: The line card 7600-ES+ on a Cisco 7600 series router may reload due to memory corruption.

  Conditions: One of the conditions is cable pull with scaled configurations. This is seen with VPLS configuration only so far. This is a rare situation and seen only once.

  Workaround: Shut the port on which OIR is done.

- CSCte99481

  Symptoms: After SSO if you get drop for around 30 secs having VPLS and 4k HWIBDS.

  Further Problem Description: After switchover the process which clears the counters for HWIDBS take the whole of CPU and not allowing OSPF to work properly. Resulting in the drop of traffic.

- CSCti78408

  Symptoms: %SYS-DFC4-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs (4/3),process = console_rpc_server_action.

  %SYS-DFC4-2-WATCHDOG: Process aborted on watchdog timeout, process = console_rpc_server_action.

Conditions: This issue can be seen with the following conditions:

1. Issuing **show tech** command on ES+
2. Issuing **show platform hardware config-pld** command on ES+

Workaround: Do not use **show tech** and **show platform hardware config-pld** commands on ES+.

Resolved Caveats—Cisco IOS Release 12.2(33)SRD3

Cisco IOS Release 12.2(33)SRD3 is a rebuild release for Cisco IOS Release 12.2(33)SRD. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRD3 but may be open in previous Cisco IOS releases.

- CSCee63182

  Symptoms: A Cisco router may crash or may stop responding.

  Conditions: This has been always seen with an atm interface only when a rate-limit command is enabled on the interface. The crash occurs when an interface that is configured with a **rate-limit** command is deleted by entering the **no interface** command and then reenabled by entering the **interface** command.

  Workaround: Remove the rate-limit configuration from the interface before deleting the interface.

  Further Problem Description: Happens under very specific circumstances and the crash is seen randomly.

- CSCse15495

  Symptoms: The following CLASS-BASED-QOS-MIB counters are incorrect in output direction:

  - cbQosCMPrePolicyByte64

  - cbQosCMPostPolicyByte64

  In input direction cbQosCMDropByte64 is incremented and is always equal to cbQosCMPrePolicyByte64.

  Conditions: Hardware specific setup: SIP-600 and 10GE SPA.

  Workaround: There is no workaround.

- CSCse29527

  Symptoms: A Cisco 7600 Series router or Cisco Catalyst 6500 Switch may unexpectedly reload due to bus error when running **remote command switch show mmls met**.

  Conditions: Occurs when the device is doing multicast.

  Workaround: Do not run the command.

- CSCse97873

  Symptoms: Resilient Ethernet Protocol (REP) flaps due to excessive CPU utilization occurs.

  Conditions: Occurs in a Resilient Ethernet Protocol (REP) segment if 4000 VLANs are configured on the router and if VLANs are allowed on a switchport.

  Workaround: There is no workaround.

- CSCse99958

  Symptoms: A Cisco router may fail to access a flash card after formatting it, and the following error message is generated:

  ```
  *** Emulating mis-aligned load at 0x80000190 PC = 0x8001179c ... succeeded
  ```

Conditions: The symptom is observed on a Cisco 7200 series, Cisco 7301, and Cisco 7500 series that run Cisco IOS Release 12.4(10) or Release 12.4(12) and occurs only when a flash card is accessed from the ROMmon prompt.

Workaround: There is no workaround. Note that the symptom does not occur in Release 12.4(8a) or an earlier release.

- CSCsh54161

  Symptoms: Under certain unusual circumstances, routes can go SIA in an EIGRP network and create transient routing loops.

  Conditions: When the metric on an interface increases rapidly, the symptom can occur. This can happen with MANET interfaces as well as bundled interfaces (such as port-channels).

  Workaround: There is no workaround.

- CSCsl01427

  Symptoms: The following symptoms all relate to the same root cause:

  1. In syntax check mode, if there is a standby in SSO mode, the **cts dot1x** command does not work and the following error messages are displayed:

     ```
     RouterRP(syntax-if)#cts dot1x %ERROR: Standby doesn't support this command ^ %
     Invalid input detected at '^' marker.
     ```

     ```
     RouterRP(syntax-archive)#path disk0: %ERROR: Standby doesn't support this command ^
     % Invalid input detected at '^' marker.
     ```

  2. After a redundancy force-switchover, the applet configuration is lost and retains only the applet name. (This is done by configuring an applet on the main RP and switchover to the Standby by issuing a redundancy force-switchover. Issue the **sh run** command on the Standby which is now the main RP.) All the action statements are lost.
  3. The Standby switch reloads by itself after going into the event manager applet configuration mode:

     ```
     Config Sync: Line-by-Line sync verifying failure on command: event manager applet
     cli-test-01 due to parser return error
     ```

  4. The Standby switch may also reload upon removing the command **event manager applet**:

     ```
     RouterRP(config)#event manager applet 1 EEM: Applet 1 is currently being modified
     ```

     OR

     ```
     RouterRP(config)#no event manager applet 1 EEM: Applet 1 is currently being
     modified
     ```

  Conditions: The symptoms are observed in syntax check mode, if there is a standby in SSO mode.

  Workaround: There is no workaround.

- CSCsl33908

  Symptoms: The image name displayed in **show version** will be truncated to 64 characters if the image name is more than that.

  Conditions: It occurs in High Availability (HA) setup.

  Workaround: There is no workaround.

- CSCsl66427

  Symptoms: Shortly after replacing FlexWAN, SNMP queue starts to fill and SNMP queue full error message is printed:

  %SNMP-3-INPUT_QFULL_ERR: Packet dropped due to input queue full

  Conditions: Occurs on a Cisco 7600 router running Cisco IOS Release 12.2(33)SRD1.

Workaround: Apply following view:

snmp-server view Flash iso included

snmp-server view Flash ciscoFlashMIB exclude

snmp-server view Flash ciscoFlashDevice exclude

snmp-server view Flash ciscoFlashPartitions exclude

snmp-server view Flash ciscoFlashPartitionTable exclude

snmp-server view Flash ciscoFlashPartitionEntry exclude

snmp-server community <name> view Flash RW

If this is not enough to get rid of SNMP queue full, reload the router so that the view applies at the router bootup.

- CSCsm26063

  Symptoms: Router crashes following a **shut/no shut** on the main interface.

  Conditions: Occurs on a router running Cisco IOS Release 12.2SXH2a. IPv6 traffic must be flowing over the WAN interface for multiple IPv6 prefixes. The crash occurs when a **shut/no shut** is done on the main interface on which multiple subinterfaces have been configured and IPv6 routing is enabled.

  Workaround: There is no workaround.

- CSCsm85890

  Symptoms: When there are two PA-2T3 cards on a VIP6-80 and hard loop one port on one PA-2t3, it causes the port on the second PA-2T3 card to flap. The impact of the issue is that the interface flaps once and it results in dropping of 6-7 packets.

  Conditions: When we do a **shut/no shut** on a serial port, the other serial port on the same VIP might flap once.

  Workaround: Put each PA-2T3 card on different VIP modules.

  Further Problem Description: Any Cisco IOS release that incorporates CSCsj96781 will definitely see this bug. The other affected serial port can belong to the same PA (in case of two-port T3+ PA) or it can belong to a different PA on a different bay but on same VIP.

- CSCso29141

  Symptoms: A Catalyst 6500 switch with an etherchannel spanning multiple DFC modules may drop packets for a certain MAC on egress. This happens when one of the DFCs carrying the etherchannel has an incorrectly programmed MAC address entry, pointing at the internal drop index.

  Conditions: This only occurs in an asymmetric routing scenario, where frames are constantly egressing the etherchannel destined for certain MAC addresses, but frames are not consistently seen from those MAC addresses. This is often the case when Hot Standby Routing Protocol (HSRP) is running, and this particular switch is the HSRP standby.

  Workaround: Through tweaking ARP and MAC address aging timers, this situation can be avoided. We recommend that the MAC address aging timer be set at least 3 times higher than the ARP timer for the VLAN interface.

  The configuration for this is:

  Switch(config)#**mac-address synchronize**

  Switch(config)#**mac-address aging-time 900**

  Switch(config)#**interface Vlan360**

Switch(config-if)#**arp timeout 300**

Further Problem Description: While a MAC address is in this condition, the following outputs will look like this:

Switch#**show mac-address-table address 0000.0000.0001 all det**

MAC Table shown in details ==

PI_E RM RMA Type Alw-Lrn Trap Modified Notify Capture Flood Mac Address Age Pvlan SWbits Index XTag

----+---+---+----+-------+----+--------+------+-------+------+--------------+----+------+------+------+----

Module 1: No No No DY No No Yes No No No 0000.0000.0001 0x3A 360 0 0x7FFF 0 Active

Supervisor: No No No DY No No Yes No No No 0000.0000.0001 0x69 360 0 0x342 0

Here, we see that the MAC address is not present on Module 2, which it should be. On Module 1, we see that the index pointed to is 0x7FFF, which represents the internal drop index in the 6500. Also, we see the "Flood" bit is set to 'No'. In this condition, all frames egressing Module 1 for this MAC will be dropped. Had "Flood=Yes", the frames would be flooded instead of dropped, which is normal behavior.

- CSCso42210

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

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

  Workaround: There is no workaround.

- 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.

- CSCsq71492

  Symptoms: A Cisco IOS device may reload with an address error or have alignment errors and tracebacks such as %ALIGN-3-SPURIOUS or %ALIGN-3-TRACE

  Conditions: The symptoms are most likely to occur when the TACACS+ server (ACS) sends an "authentication error" when ACS is configured, or when a request timeout occurs. There may be other AAA or TACACS related conditions that cause the symptom.

  Workaround: There is no workaround.

- CSCsq82041

  Symptom: Memory leak when remote PEs have more xconnects configured than UUT

  Conditions: set session limit under vpdn-group and over subscribe sessions. Workaround: NA

- CSCsq84624

  Symptoms: A Cisco router might crash when **debug condition portbundle ip 10.1.1.1 bundle 0** is configured.

  Conditions: Occurs when this command is executed prior to configuring **ip portbundle**.

  Workaround: There is no workaround.

- CSCsr06094

  Symptoms: A Cisco router may ungracefully reload.

  Conditions: The symptom is observed when the router is processing CoA RADIUS messages and when certain debugs are turned on.

  Workaround: Disable all debugs.

- 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.

- CSCsr75700

  Symptoms: In very rare cases, a Cisco 10000 series router crashes with a log similar to:

  %Software-forced reload Breakpoint exception, CPU signal 23, PC = 0x408FAFC0

  Possible software fault. Upon recurrence, please collect crashinfo, "show tech" and contact Cisco Technical Support.

  -Traceback= 408FAFC0 408F8B78 41990010 419910E0 41992DB8 42158AF4 41992EC0 41953F8C 41956C1C

  (Note that the hex values of the traceback may be different.)

Conditions: The symptom is observed on a Cisco 10000 series router that is running Cisco IOS Release 12.2(33)SB1.

Workaround: There is no workaround.

Further Problem Description: The occurrence of the problem so far has been rare. The decode of the traceback points to a BGP issue. The confirmation of whether a crash is due to this bug in BGP or not can only be made after the traceback from the crash has been decoded by Cisco support engineers.

- CSCsr88705

  Symptoms: Redistributed routes are not being advertised after a neighbor flap.

  Conditions: This symptom is observed if BGP is redistributing local routes and if there are multiple neighbors in the same update-group and then a neighbor flaps. For the flapped neighbor, some redistributed routes are not being advertised.

  Workaround: Undo and redo the redistribution.

- CSCsr90248

  Symptoms: Changing any of the parameters of a route-map does not take effect.

  Conditions: Occurs when using a BGP aggregate-address with an advertise map.

  Workaround: Delete the aggregate-address statement and then put it back for the change to take effect.

- CSCsu11668

  Symptoms: A router configured with BGP import from the global IPv4 table into a VRF using the VRF configuration command **import ipv4 unicast map ...** may exhibit a brief traffic outage to destinations reached through the imported routes following a switchover.

  Conditions: Global to VRF import must be configured under the VRF. Issue only affects Cisco IOS Release 12.29(33)SR releases.

  Workaround: There is no workaround.

- CSCsu26526

  Symptoms: Memory leak can be seen on the LNS.

  Conditions: The symptom is observed on the L2TP Network Server (LNS) when the PPP client does a renegotiation.

  Workaround: There is no workaround.

- CSCsu49189

  Symptoms: Frame-Relay fragment output not seen when modifying the attached map-class.

  Conditions: Occurs on a Cisco 7200 router.

  Workaround: Detach and attach Frame-Relay fragment.

- CSCsu72059

  Symptoms: After multiple OIRs, memory gets fragmented in line card and at one stage the mallocs start failing.

  Conditions: There is a higher chance of fragmentation when we have ATM OC3 SPAs in both the bays and huge configurations which eat up lot of memory.

  Workaround: Reload the line card.

- CSCsu74400

Symptoms: A device running FTP to transmit the DHCP database may experience a file descriptor leak that results in errors such as:

ROUTER#show run

OR

ROUTER#show start Using XXXX out of XXXX bytes %Error opening nvram:/startup-config (Bad file number)

OR

ROUTER#dir nvram: Directory of nvram:/ %Error opening nvram:/ (File table overflow) XXXX bytes total (XXXX bytes free)

Conditions: Occurs when the router is configured to use FTP to transmit the DHCP database:

ip dhcp database ftp://XXXX:XXXX@X.X.X.X/XXXX

And the FTP server becomes unreachable. The file descriptor leak can be viewed in the output of **show file descriptors**:

ROUTER-B#show file descriptors File Descriptors:

FD Position Open PID Path 0 0 0302 145 ftp://X.X.X.X/DHCP 1 0 0302 145 ftp://X.X.X.X/DHCP 2 0 0302 145 ftp://X.X.X.X/DHCP 3 0 0302 145 ftp://X.X.X.X/DHCP 4 0 0302 145 ftp://X.X.X.X/DHCP 5 0 0302 145 ftp://X.X.X.X/DHCP 6 0 0302 145 ftp://X.X.X.X/DHCP 7 0 0302 145 ftp://X.X.X.X/DHCP 8 0 0302 145 ftp://X.X.X.X/DHCP 9 0 0302 145 ftp://X.X.X.X/DHCP <snip>

Workaround: Ensure that the FTP server does not become unreachable for more than 128 total minutes, as there are only 128 file descriptors. In the event that all 128 file descriptors are leaked, a reboot is required to recover.

- CSCsu79754

  Symptoms: PIM packets may be processed on interfaces which PIM is not explicitly configured.

  Conditions: Unknown at this time.

  Workarounds: Create an ACL to drop PIM packets to such interfaces.

- CSCsv07467

  Symptoms: When doing IP session on Layer 4 Redirect with VPN routing/forwarding (VRF) web logon scale test, subscriber tries to authenticate with 20 characters per second from test tool. MCP crashed into ROMMon

  Conditions: Occurs only when test tool sends authentication at 20 characters per second

  Workaround: There is no workaround.

- CSCsv21612

  Symptoms: High CPU on PM callback process on SP. Depending on the number of trunk links configured, the high CPU time increases exponentially with the number of trunk links.

  Conditions: This occurs when VTP pruning is enabled and there are too many trunk links. High CPU on PM callback process is normal as the switch is pruning the VLANs. Problem only occur when there are too many trunk links and the high CPU last for too long and affects other layer 2 operations.

  Workaround: Disable VTP pruning or reduce the number of trunk links. For phones, use mode access with voice VLAN configured if this configuration is supported by phone.

- CSCsv27372

  Symptoms: GRE tunnel terminates on switch where Server Load Balancing (SLB) is configured. Traffic to SLB VIP and real server fails and causes crash.

Conditions: Occurs on a router running Cisco IOS Release 12.2(33)SRC2. Router crashes and creates core dump while doing a telnet to a real server under NAT-configured server farm using GRE Tunnel.

Workaround: There is no workaround.

- CSCsv38225

  Symptoms: Router may reload when you unconfigure and then configure the **ipv multicast-routing** commands in quick succession.

  Conditions: Occurs when these commands are entered in quick succession, such as with copy and paste.

  Workaround: Allow for a delay when entering the commands **ipv multicast-routing** and **no ipv multicast-routing**.

- CSCsv43802

  Symptoms: System crashes while running online diags.

  Conditions: The system may crash when there is a spike in CPU utilization or traffic in the system.

  Workaround: There is no workaround.

- CSCsv61073

  Symptoms: BGP neighbors may experience increased flapping.

  Conditions: Occurs when large number of BGP neighbors are configured with aggressive BGP hold-timer values.

  Workaround: Increase the BGP hold-timer values beyond 10/30.

- CSCsv62777

  Symptoms: VTY session may get stuck after some extended pings are done and the CPU process may go high.

  Conditions: The symptom is observed when an extended ping with CLNS is done and the command is left incomplete until the vty session times out.

  Workaround: Issue can be prevented by not leaving the extended 'ping clns' command incomplete for long time in the vty session.

- CSCsv90106

  Symptoms: A router may write a crashinfo that lacks the normal command logs, crash traceback, crash context, or memory dumps.

  Conditions: This might be seen in a memory corruption crash depending on precisely how the memory was corrupted.

  Workaround: There is no workaround.

- CSCsw16157

  Symptoms: Routers using OSPF and MPLS Traffic Engineering may crash or operate incorrectly following changes to the configuration of MPLS-TE tunnel interfaces or OSPF. In some cases a configuration change will cause an immediate crash, while in others memory may be corrupted resulting in problems later.

  Routers using MPLS-TE primary auto-tunnels are particularly vulnerable because those tunnel interfaces may be removed as the result of network topology changes as well as by modifying the running configuration.

Conditions: In order to be exposed to this problem, a router must have MPLS TE tunnel interfaces that are announced to OSPF. Systems that do not run OSPF, or which do not use MPLS-TE are not affected.

Systems that operate without "service alignment detection" enabled may crash when the following configuration commands are issued:

Global configuration mode:

* no interface tunnel <n> * no router ospf * no mpls traffic-eng auto-tunnel

Interface configuration mode:

* no ip unnumbered * no ip address

Exec mode:

* clear mpls traffic-eng auto-tunnel

Note that routers running modular IOS (ION) and IOS-XE do not have alignment detection enabled.

Regardless of the state of alignment detection, removing the last MPLS-TE tunnel interface to a destination can cause problems, as can removing auto-tunnel configuration. Removal of dynamically created auto-tunnel interfaces as a result of changes in the network topology has the same effect.

Note that routers using auto backup tunnels to provide fast reroute for static MPLS-TE tunnels do not have any extra exposure to this bug because while these backup tunnels may be removed due to topology changes, the static tunnel to the same destination will not be.

Normal UP/DOWN state changes of tunnel interfaces do not cause problems.

Workaround: To remove a MPLS-TE tunnel interface, first configure it down with the "shutdown" command in interface submode.

To remove an OSPF instance, first disable MPLS-TE for the instance by configuring "no mpls traffic-eng area <n>" in router ospf submode.

No workaround is available for MPLS-TE auto-tunnels.

- CSCsw25200

  Symptoms: When flapping a fiber, the link protocol comes up, but the line protocol does not.

  Conditions: Occurs on links between SIP modules.

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

- CSCsw39190

  Symptoms: Both active and standby supervisors crash.

  Conditions: Occurs when Control Plane Policing (COPP) is configured and there are multiple session churns happening with PPPoE subscribers.

  Workaround: There is no workaround.

- CSCsw48359

  Symptoms: With traffic flowing normally over a GRE tunnel terminating on the ES20 line card the module will crash when IPSec tunnel protection is enabled.

  Conditions: Occurs when tunnel endpoint is an interface on the ES20 line card.

Workaround: This crash is seen only when GRE is accelerated by spa-ipsec-2g. If GRE is accelerated by the SUP, the crash does not happen. This is done by default in VRF mode without any other directives like "crypto engine mode gre vpnblade". To ensure the tunnel is adding "crypto engine gre supervisor" in the global configuration mode and on all the tunnels that are handled by ES20 for mpls recirculations.

As an alternative workaround, If the customer wants the GRE acceleration to be taken over by the spa-ipsec-2g. An ACL needs configured to drop all the plain unencrypted GRE traffic between a tunnel's source and destination ip addresses may also be effective if applied prior to configuring the "tunnel protection ..." command. However, this workaround may not scale in certain configurations.

As a preventive precautionary measure. A safer practice would be to configure the Customer Edge device prior to configuring the Provider Edge. This configuration order should prevent this issue from occuring when adding IPSec Tunnel protection to GRE Tunnels.

- CSCsw50069

  Symptoms: Microflow policing fails to be removed or modified on port-channel subinterface.

  Conditions: Occurs on a Cisco 7600 series router with port-channel subinterface configured for microflow policing, and the same policy configured on subinterface with encap VLAN as well as another subinterface without encap VLAN.

  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.

- CSCsw76817

  Symptoms: Whenever MTU is configured under a port-channel with EVC (Ethernet Virtual Circuit), the MTU functionality does not work as expected.

  Conditions: This happens only with Layer 3 port-channels.

  Workaround: There is no workaround.

  Further Problem Description: Whenever a member link is added to a port-channel, the member link's MTU is programmed to the jumbo MTU value (default 9216). Even when a custom MTU value is configured under port-channel, all the member links' MTUs are programmed with 9216.

- CSCsw93867

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

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

  bandwidth of 24.00% is not available (1.00%)

  bandwidth of 24.00% is not available (1.00%)

  bandwidth of 24.00% is not available (1.00%)

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

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

- CSCsx03301

  Symptoms: Crash in TCP.

  Conditions: Happens when clearing a BGP neighbor. The trigger is uncertain and hard to reproduce.

  Workaround: There is no workaround.

- CSCsx07159

  Symptoms: A policy-map is applied to an interface on ESM20G card and has a **random-detect aggregate** action configured in a class. If another class is added to the policy-map which has match statement as "match cos <cos-value>", this class gets added. Now if **random-detect aggregate** is removed from the previous class, an error message is dumped on screen :

  'match cos' combined with other match statements at the same class level is not supported for this interface.

  If random-detect action is added to this class, router crashes.

  Conditions: Occurs with the following configuration:

  policy-map PMAP_UPLINKS

  class CMAP-RT-COS (match cos <vaue>)

  class CMAP-BC-EXP

  no random-detect aggregate

  random-detect -----> (CRASH)

  Workaround: Do not add a class-map with "match cos" filter to a policy-map which conflicts with other class-map filters.

- CSCsx07537

  Symptoms: Delay in bootup time of the line cards occurs during reload with diags enabled. Issue not seen when diags are disabled.

  Conditions: There is no specific configuration or traffic combination that will trigger this issue. Issue seen with or without any Ethernet Virtual Circuit (EVC) configs or traffic conditions.

  Workaround: Disable bootup diags or power down the 6748-GE-TX card

- CSCsx08861

  Symptoms: ATOM VC status is seen as down in standby RP and traffic loss is seen after switchover for 44 seconds.

  Conditions:

  1. Bring 6RU up (SSO) with 1 AToM VC, 1 AToM VP (Initial VC state: active:UP; standby:HOTSTANDBY)

  2. Delete the AToM VC sub-int ('no int a2/2/0.122') and delete the AToM VP sub-int ('no int a2/2/0.1001')

  3. Re-configure back the same AToM VC and VP configuration (VC state: Active:UP; Standby:DOWN for AToM VC)

4. If I do a force switchover (’redundancy force-switchover’). It will experience ~44 seconds of traffic lost for this VC.

Workaround: There are two work around for this issue:

1. Do not reconfigure the ATOM VC immediately after deleting a subinterface.

2. Do not copy and paste the ATOM VC configuration. Either do it manually step by step or copy the configuration from a file.

- CSCsx09343

  Symptoms: PKI daemon is stuck in DNS resolution attempt for the hostname used in the CDP.

  Conditions: The when symptom is observed using name resolution for automatic actions taken by the router during non-interactive sessions (CRL download using name in CDP URI). Only applicable if ’ip domain-lookup’ is enabled within the config

  Workaround: There is no workaround.

- CSCsx10086

  Symptoms: When trying to configure a peer template using the command **template peer-session** *S1_1* under **router bgp** *1* , it enters into UNKNOWN-MODE. Once there, we cannot get out of that mode and the router has to be rebooted.

  Conditions: The bug is seen only in Cisco ION images. Cisco IOS images are fine. Following is an example:

  ip39-1(config)#router bgp 1

  ip39-1(config-router)#template peer-session S1_1

  ip39-1(UNKNOWN-MODE)#?

  % Unrecognized command

  ip39-1(UNKNOWN-MODE)#end ^ % Invalid input detected at ’^’ marker.

  Workaround: There is no workaround.

- CSCsx15138

  Symptoms: Device crashes upon entering command **sh policy-map interface**.

  Conditions: Unknown at this time.

  Workaround: There is no workaround.

- CSCsx34584

  Symptoms: Crash is seen when 1000 IP sessions identified by same MAC address are setup and torn down using Cisco Intelligent Services Gateway (ISG).

  Conditions:

  1. Setup 1000 IP sessions on ISG on one port. 2. Setup another 1000 sessions on second port with same MAC address range as in first port. 3. Ensure 1000 sessions are up. The other 1000 sessions setup request would be rejected as they are using the same MAC address as in step 1. 4. Clear the 1000 sessions using **clear sss session all**. 5. Repeat steps 2, 3, and 4 until crash is seen.

  Note: This scenario is not supported and has been documented. Please refer to the Restrictions section on the following URL:
  http://www.cisco.com/en/US/docs/ios/isg/configuration/guide/isg_sub_aware_enet.html#wp1074579

Workaround: This is a negative test case and will never happen in practical setups as the MAC addresses will not overlap. Also the network topology should ensure that the same subscriber MAC address does not appear on more than one physical interface.

- CSCsx46415

  Symptoms: Virtual Private LAN Services (VPLS) unicast traffic not flowing over the VC when core-facing port is ESM20 line card.

  Conditions: Core-facing port must be on the 9th slot or higher in a Cisco 7609 or Cisco 7613 chassis. Also the VC neighbor scale should be very high on that VPLS VLAN.

  Workaround: Use slots lower than 9.

- CSCsx49573

  Symptoms: Three separate Cisco IOS Hypertext Transfer Protocol (HTTP) cross-site scripting (XSS) vulnerabilities and a cross-site request forgery (CSRF) vulnerability have been reported to Cisco by three independent researchers.

  The Cisco Security Response is posted at the following link:
  http://www.cisco.com/warp/public/707/cisco-sr-20090114-http.shtml

  Conditions: See "Additional Information" section in the posted response for further details.

  Workarounds: See "Workaround" section in the posted response for further details.

- CSCsx55152

  Symptoms: Switch does not send TC trap if it is not a root bridge

  Conditions: If switch is a root bridge, it generates TC trap when link goes both up and down. But if switch is not a root bridge, it generates TC trap only when link goes up.

  Workaround: There is no workaround.

- CSCsx58335

  Symptoms: When relaying to multiple servers from an unnumbered interface, the DHCP relay sends packets to all servers, even for packets where the client is in a RENEWING state unicasting to attempt to reach a single server. ARP entries are retained for all offered addresses, even if the client is ultimately using a different address. These extra ARP entries persist for several hours.

  Conditions: The symptom is observed under the following conditions:

  1. When relaying a DHCP packet on an unnumbered interface and the DHCP client is in a renewing state (as determined by the fact that the packets are sent to the DHCP server which allocated the address so that we do not end up giving the client a new address, which would then interrupt the user sessions).
  2. When the client is in any other state, or if we do not get a response from the DHCP server, the packets are sent to all helper-addresses.

  Workaround: Use Cisco IOS 12.4T images.

  Further Problem Description: Only retain an ARP entry for the address that the DHCP client ACKs. Do not retain addresses offered by DHCP servers which the client did not use in the ARP table.

- CSCsx67931

  Symptoms: The **no l2tp tunnel authentication** command does not work at LNS.

  Conditions: This symptom happens when the VPDN group that is used has a **virtual-template** *x*.

  Workaround: Configure the **no l2tp tunnel authentication** command under virtual template.

- CSCsx81707

Symptoms: Following error message are seen when the **frame-relay fragment** <*fragment size*> command is configured under map-class attached to PVC:

% Fragment size 110 not supported. Supported fragment size are 128, 256 and 512. Rounding current fragment config to 128.

Conditions: This seen in distributed platforms (Cisco 7600) when fragment size configured is not 128, 256, or 512.

Workaround: Configure the fragment size as 128, 256 or 512

- CSCsx93845

  Symptoms: Memory leak is seen on configuring and unconfiguring "cem-group".

  Conditions: Occurs when configuring and unconfiguring 4 "cem-groups" per controller.

  Workaround: There is no workaround.

- CSCsx95338

  Symptoms: Crash occurs when BGP configuration is removed.

  Conditions: BGP is checkpointing routes to the redundant RRP when the configuration change occurs. More likely to occur in a scaled setup.

  Workaround: Do not enter the **no router bgp** command.

- CSCsy03758

  Symptoms: VPN routing/forwarding (VRF) transfer fails.

  Conditions: Occurs when ISG is configured on the device.

  Workaround: There is no workaround.

- CSCsy07555

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCsy07953

  Symptoms: Any attempt to copy a file from a router to an FTP server will fail. The FTP error is "No such file or directory".

  Conditions: This is only a problem with FTP and only when transferring to an FTP server. Transfers from an FTP server work as expected.

  Workaround: Use a different file transfer protocol, such as TFTP.

- 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

- CSCsy19659

Symptoms: When using Point-to-Point Tunnelling Protocol (PPTP) with RADIUS Accounting, there may be several "nas-error" and "lost-carrier" listed in accounting as the Acct-Terminate-Cause.

Conditions: The symptom is observed when using Cisco IOS Release 12.4T (Releases 12.4(15)T-12.4(22)T confirmed) and using PPTP with RADIUS Accounting in place.

Workaround: There is no workaround.

- CSCsy21885

  Symptoms: After SPA reload, the CHOC12-DS0 SPA may be transmitting B1/B2/B3 errors out. Remote side will detect SF BER, B1 TCA, B2 TCA, or B3 TCA alarms, or DS3 or DS1 alarms. The CHOC12-DS0 SPA will have SONET line REI, Path REI or DS3/DS1 RAI alarm.

  Conditions: When the SPA boots up during temperature transition, the SPA transmit side could trigger B1/B2/B3 error detected by remote end. In a stable temperature environment, this problem is hard to reproduce. After SPA is booted up, the problem can not be reproduced even if temperature transits.

  Workaround: A software workaround was released in Cisco IOS Release 12.2(33)SRD1 to reduce the issue. But in some SPAs, the problem may still happen. When the problem happens, reload the SPA.

- CSCsy24878

  Symptoms: Bulk sync fails.

  Conditions: Occurs when the **relay destination** command is configured on the device.

  Workaround: There is no workaround.

- CSCsy26883

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

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

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

- CSCsy29534

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

  Conditions: It was observed in the following context:

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

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

- CSCsy32000

  Symptoms: Router crashes when BGP-IPv6 directly connected IBGP neighbors receives route with Link-local Nexthop.

  Conditions: BGP sends IPv6 link-local address in following cases:

  1) Directly connected eBGP neighbors

  2) BGP Ipv6 neighbors connected using Link-local address

In case of this defect, testing device is advertising link-local nexthop for directly connected neighbor using global IPv6 address. Cisco router will never advertise link-Local nexthop.

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.

- CSCsy53076

  Symptoms: Copy to "slavedisk:" is failing with the following error:

  Error writing slavedisk0:/rsp72043-adventerprisek9_dbg-mz.122-33.0.5.SRD (TF I/O failed in data-in phase)

  Conditions: The issue is seen in RPR mode with Cisco IOS Release 12.2SR rsp720 image.

  Workaround: Copy the file in SSO mode.

- CSCsy54365

  Symptoms: In extremely rare conditions, traffic loss might be observed through ws-x6704 modules equipped with DFC (DFC3b & 3bxl, DFC3a)

  Conditions: To confirm that traffic loss might be related to this issue use the following command:

  remote command module *mod#* **show platform soft earl reset history**

  where <mod#> is slot number of the module experiencing traffic drops (ingress module)

  cat6500#**remote command mod 11 sh platform soft earl reset history**

  Num. of times patch applied : 156

  Num. of times patch requested : 156

  Time Reason InProgress Data

  ----------+----------+----------+----------

  5d20h Non-Earl Fatal error 0000 1701FFFFFFFFFFF

  5d20h Non-Earl Fatal error 0000 1701FFFFFFFFFFF

  5d20h Non-Earl Fatal error 0000 1700FFFFFFFFFFF

  5d20h Non-Earl Fatal error 0000 1700FFFFFFFFFFF

For traffic loss to be related to this issue in above output one should see lines similar to above (most important is the last part i.e. 1701FFFFFFFFFFF and 1700FFFFFFFFFFF). There should be multiple lines like this and new lines might appear from time to time. Traffic loss would coincide with the appearance of new lines.

Workaround: There is no workaround other than upgrading to a release that has been fixed.

- 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).

- CSCsy60498

  Symptoms: On RSP720-10GE, VPNSPA always remains in INIT state.

  Conditions: Unknown at this time.

  Workaround: There is no workaround.

- CSCsy60668

  Symptoms: On a router in which MPLS Traffic Engineering (TE) is configured, toggling the router-id in the router configuration can cause the router to reload. For example, configuring "router ospf 100 mpls traffic-eng router-id loopback 0" quickly followed by "mpls traffic-eng router-id loopback 1" may trigger this symptom.

  Conditions: It is necessary that "mpls traffic-eng tunnel automesh" is running in the OSPF area of the router, although automesh need not be configured on the affected router.

  Workaround: There is no workaround.

- CSCsy60846

  Symptoms: With 2X1GE-V2 SPA on SIP400, when the interface connector changes from SFP to RJ45, the port failed to be up and it could no longer ping its partner.

  Conditions: When the media-type of the 2X1GE-V2 interface is chanaged to RJ45 using the **media-type rj45** command, the interface goes to down state. This issue is found in Cisco IOS Release 12.2(33)SRB, SRC, and SRD.

Workaround: Reload the router to bring up RJ45 ports.

- CSCsy61006

  Symptoms: Lawful intercept users are appearing in output from **show run**.

  Conditions: Occurs in Cisco IOS Release 12.2(33)SRC.

  Workaround: There is no workaround.

- CSCsy62160

  Symptoms: VLAN state unable to recover after shutdown by "mac-limit."

  Conditions: Applicable for extended VLAN after MAC limit exceeded and action configured to shutdown.

  Workaround: There is no workaround.

- CSCsy70184

  Symptoms: Traceback occur on SPA inside SIP-400.

  Conditions: Occurs during online insertion and removal (OIR) of SPA.

  Workaround: There is no workaround.

- CSCsy73123

  Symptoms: Connected route on port-channel sub-interface is not removed when port-channel is down.

  Conditions: Happens when using /22 subnet. Does not happen when using /24 subnet.

  Workaround: There is no workaround.

- CSCsy74334

  Symptoms: Sticky-ARP entries are refreshed forever even after the client is removed from the network.

  Conditions: This issue is seen after an upgrade from Cisco IOS Release 12.2(33)SRB5 to Release 12.2(33)SRD1.

  Workaround: There is no workaround.

- CSCsy77191

  Symptoms: Native GigE interfaces of a Cisco 7200 NPE-G2 router will not acknowledge reception of pause frames and will not stop its transmission in case of media-type RJ45.

  Conditions: The symptom is observed with media-type RJ45 and with SFP with "no neg auto" configured.

  Workaround: There is no workaround.

  Further Problem Description: There are no issues with SFP with a "neg auto" configuration.

- CSCsy77298

  Symptoms: Option 82 is not appended in DHCP NAK packet by DHCP server.

  Conditions: Not any specific condition.

  Workaround: There is no workaround.

- CSCsy81519

  Symptoms: ISG subnet session feature if used in an environment where subscribers are connected to ISG interface on Layer 2 cloud, that is, ISG is the default gateway for the subscribers yet ISG subscribers interface is in routed mode, then adjacency to these connected subscribers is removed

as soon as a subnet session is created and next hop is installed for these subscribers as the logical network id computed using the framed subnet mask received from AAA server as access accept radius attribute.

Conditions: This condition will occur for subnet session feature in scenario where ISG interface is defined under routed mode; however subscribers are connected over layer-2 cloud to this ISG interface, that is, ISG is the default gateway for these subscribers.

Workaround: There is no workaround if the subnet session feature has to be deliberately used in scenario as defined under conditions above. However this problem will not occur if the subscribers are one hop or more away from ISG.

Further Problem Description: ISG subnet session feature is used to group a number of sessions together using IP framed netmask attribute. The ISG subnet session feature can be used if ISG interface is defined under routed mode.

For example IP addresses belonging to a client say 192.168.0.68/24, 192.168.0.69/24, 192.168.0.70/24 and 192.168.0.70/24 can be grouped together under one ISG session if at the time of session creation a IP framed netmask 255.255.255.252 is returned in the access accept message from AAA server. The subscribers are one or more hop away from ISG interface (10.10.10.1/24)

The IP Framed Netmask attribute is used to compute the range of IP addresses to be grouped together under one ISG session. In example above, if a session is initiated firstly by IP address 192.168.0.69/24; then using IP Framed Netmask the computed range of IP addresses to be grouped together will be 192.168.0.68 to 192.168.0.71.

Now in a scenario where ISG interface is defined under routed mode though the subscribers are connected directly over Layer 2 cloud to ISG interface and Subnet Session is required to be used as a feature; then the stated problem under section Symptom above will occur.

Using example above and applying to this problematic scenario - the IP addresses of client 192.168.0.68/24, 192.168.0.69/24, 192.168.0.70/24 and 192.168.0.70/24 have to be grouped together under one ISG session using Subnet Session feature by returning a IP Framed Netmask 255.255.255.252 under Access Accept from AAA server, however the ISG interface (192.168.0.1/24) in this scenario is the default gateway to these Client IP end points.

Now as soon as the session is created and authenticated and Subnet Session feature is installed the next hop for these IP range 192.168.0.68 to 192.168.0.71 computed using IP Framed Netmask value 255.255.255.252 would be 192.168.0.68/30 resulting in traffic destined to all the range of IP addresses grouped under Subnet Session forwarded to 192.168.0.68/30 instead of using ARP to reach the IP end points directly.

- CSCsy84862

  Symptoms: In a rare event, router may crash in EIGRP code after a peer bounce and route removal.

  Conditions: Crash seen during EIGRP route updates.

  Workaround: There is no workaround.

- CSCsy85171

  Symptoms: Switch reports following messages:

  CDL2 Read Error: Time out

  CDL2 Write Error: Time out

  Conditions: Occurs on a Catalyst 6500 switch running Cisco IOS Release 12.2(18)SXF.

  Workaround: Re-seat the X2 modules. It is highly recommended to do a complete diagnostic test on all modules.

- CSCsy86078

Symptoms: Router crashes with memory corruption.

Conditions: Occurs when BFD is configured on 10GigE interfaces and constant link flaps.

Workaround: There is no workaround.

- CSCsy88134

  Symptoms: When using an ES-40 10GE linecard, if the MAC layer of the WAN connection goes down, but the optical PCS layer remains up, the ES-40 port will never realize the link is down and will instead always keep the interface Up/Up. 10G ports in the ES+ family of line cards do not take advantage of link fault signalling by peer.

  Protocols relying on fast reconvergence, will not be able to take advantage of the 10G link fault signalling.

  Conditions: This problem can occur on any 10GE interface on an ES-40 line card when the remote transceiver or repeater keeps the PCS layer up but takes the MAC layer down.

  The Link layer detection algorithm for 10G ports in the ES+ does not consider a Remote Fault signalled by the peer end. Thus link will continue to show as Link-Up, even though the remote end MAC has experienced a RX FAULT and did not happen to switch off the laser

  Workaround: There is no workaround except to rely on higher layer protocols that send hellos or keepalives to determine when the link goes down and reroute around the failure with those protocols. Line protocol will never go down when the PCS layer is up on an ES-40 line card.

- CSCsy88640

  Symptoms: A core dump may fail to write, with the following errors seen on the console:

  current memory block, bp = 0x4B5400A0,

  memorypool type is Exception

  data check, ptr = 0x4B5400D0

  bp->next(0x00000000) not in any mempool

  bp_prev(0x00000000) not in any mempool

  writing compressed ftp://10.0.0.1/testuncached_iomem_region.Z

  [Failed]

  writing compressed ftp://10.0.0.1/testiomem.Z

  [Failed]

  writing compressed ftp://10.0.0.1/test.Z

  [Failed]

  %No memory available

  Conditions: This is only seen for memory corruption crashes when "exception region-size" is configured to a value that is not divisible by 4.

  Workaround: The recommended setting for exception region-size is 262144 in newer images. In older images, where the maximum configurable value is 65536, use the maximum.

- CSCsy96407

  Symptoms: Downstream traffic stopped after delete/recover of sub-interface configuration while sessions are up.

  Conditions: Occurred with the following configuration:

  * L2access IP aggregation session

* ISG as DHCP relay

* No VPN routing/forwarding (VRF)

* TAL authentication

Workaround: There is no workaround.

- CSCsz00959

  Symptoms: Standby router reboots continuously and comes to the prompt only after second or third attempt.

  Conditions: When the standby is booting up, during the startup bulk sync, Cat6k QoS Manager client will time out after 30 seconds (depends on load on the box). Due to stress QoS config, during bulk sync, the standby is taking more time, and this triggers active to reset the standby.

  Workaround: There is no workaround.

- CSCsz01695

  Symptoms: STP network will not converge if the **vlan dot1q tag native** global command is enabled. BPDUs will not get transmitted over Virtual Private LAN Services (VPLS) pseudowire (PW).

  Conditions: Occurs in a network with nPE redundancy, where the redundant PEs are connected through VPLS PW.

  Workaround: Disable the **vlan dot1q tag native** command.

- CSCsz05181

  Symptoms: A router may reload unexpectedly.

  Conditions: The symptom is observed when the router has Bidirectional Forwarding Detection (BFD) configured and is actively sending keepalives. The crash has multiple possible triggers:

  – It can be triggered by certain show commands (**show bootvar** and **show c7200** are known to cause the problem). The issue will not be seen on every invocation of the commands. It is a rare timing condition, so the probability of the crash increases as the commands are run more frequently.

  – It can also be triggered by large scale BFD deployments (hundreds of sessions on a single router).

  Workaround: Unconfigure BFD.

- CSCsz07569

  Symptoms: The session ID changes between "interim" and "stop" accounting records.

  Conditions: The symptom has been observed on Cisco IOS Release 12.2(31)SB12 with "radius-server attribute 44 extend-with-addr" in the configuration.

  Workaround: Do not configure "radius-server attribute 44 extend-with-addr".

- CSCsz10073

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

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

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

- CSCsz11784

  Symptoms: DS3 interface on choc3/STM1 stops passing traffic.

Conditions: Occurs when a DS3 is oversubscribed.

Workaround: There is no workaround.

- CSCsz14273

  Symptoms: A Cisco IOS device may produce CPUHOG error messages and a watchdog timeout unexpected restart when running a Tool Command Language (Tcl) Embedded Event Manager (EEM) policy.

  Conditions: This occurs when the EEM policy uses the Tcl **puts** command to print a very large amount of text.

  Workaround: Do not use this command to print out a large amount of text.

- CSCsz15931

  Symptoms: The entPhysicalVendorType for Transceivers lists the vendortype of Port.

  Conditions: Occurs during normal operation.

  Workaround: There is no workaround.

- CSCsz16723

  Symptoms: A Cisco router running Cisco IOS Release 12.2(33)SRC1 may crash when removing the TE tunnel mode on a SIP600 or ES20 card.

  Conditions: A tunnel bot uses the following script to remove tunnels:

  interface Tunnel37025

  no mpls ip

  no tunnel mode mpls traffic-eng

  exit

  no interface Tunnel37025

  In the transient time between removal of tunnel mode and removing the tunnel interface, packets are still moving through EARL.

  Workaround: Shutdown the tunnel first, then complete the script:

  interface Tunnel37025

  shutdown

  no mpls ip

  no tunnel mode mpls traffic-eng

  exit

  no interface Tunnel37025

- 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 send by AAA accounting records:

  Apr 16 09:59:16.358: RADIUS: NAS-Port-Id [87] 25 "GigabitEthernet0/1.118:"

  Format sent in reply to CoA Query:

  Apr 16 10:03:49.149: 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.

- CSCsz20271

  Symptoms: HQF is not getting cleaned after a policy with priority child class is removed from the "serial-vaccess" MLP interface. Also when removing the policy, an error message is seen:

  qos-reg15-r5#config term

  Enter configuration commands, one per line. End with CNTL/Z.

  qos-reg15-r5(config)# no policy-map customer

  please remove queuing feature from child policy first

  qos-reg15-r5(config)#end

  Conditions: The priority feature cleanup fails and prevents further service policy removal.

  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.

- CSCsz21857

  Symptoms: IPV6 traffic dropped over Virtual Private LAN Services (VPLS) cloud.

  Conditions: VPLS core is configured. IPV6 end devices are PCs.

  Workaround: When routers are used as end devices instead of PCs, then the issue is not seen

- CSCsz27104

  Symptoms: Acct-Session-Id attribute received in CoA message is decoded incorrectly.

  Conditions: When session ID is less than 8 hex characters, the decoded value is incorrect.

  Workaround: There is no workaround.

- CSCsz30192

  Symptoms: Following error message is seen:

  %SIP200_MP-4-PAUSE: Non-master CPU is suspended for too long

  Conditions: This is seen when fragmentation is configured under PVC and either that configuration is changed or PVC state changes.

  Workaround: There is no workaround.

- CSCsz30221

  Symptoms: Router crashes.

  Conditions: Occurs while unconfiguring class-default.

  Workaround: There is no workaround.

- CSCsz30839

  Symptoms: Switch virtual interface (SVI)-to-SVI Layer 3 ping is failing.

  Conditions: Occurs when SVI (VLAN) is configured with IP address on both ends.

  Workaround: There is no workaround.

- CSCsz37530

  Symptoms: Port is shut down, and following error message is displayed:

  %SYS-DFC3-2-LINKED: Bad enqueue of 191C92B4 in queue FD9EAD0 -Process= "SCP Hybrid process"

  Conditions: Problem is seen with Cisco 7600 running Cisco IOS Release 12.2SRD image with Port-channel configured and the member-link used is a ES+ Linecard interface.

  Workaround: There is no workaround.

- CSCsz39086

  Symptoms: With a subinterface or software Ethernet Over MPLS (EoMPLS) configured for a single tag, QinQ traffic with outer VLAN tag matching the configuration, but with full-range of inner tag is dropped.

  Conditions: All QinQ traffic with the outer tag matching the configured tag on subinterface is dropped.

  Workaround: Use scalable EoMPLS, which provides a versatile range of VLAN matching and has the required properties as expressed in this defect.

- CSCsz40772

  Symptoms: Traffic is lost for local forwarding between two EVCs in a VRF.

  Conditions: Occurs when VRF includes attachment circuits which are defined as EVCs. Each EVC is configured on separate bridge-domain and separate IP subnet. Forwarding between remote PEs works properly but local traffic between the EVCs breaks.

  Workaround: Keep the EVC on different NPs on the ES40 or replace EVC and bridge domain configuration by sub-interfaces.

- CSCsz42143

  Symptoms: 6148A-GE-TX module resets due to keep-alive failures.

  Conditions: Excessive errors and micro link flaps on a port.

  Workaround: There is no workaround.

  Further Problem Description: This is a rare problem triggered by misbehavior of a 10Base-T hub when a FastEthernet host is connected to it.

- 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.

- CSCsz45226

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

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

  Workaround: There is no workaround.

- CSCsz45509

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

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

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

- 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

- CSCsz47517

  Symptoms: Policy-map counters are not updated after online insertion and removal (OIR), and shaping is not happening.

  Conditions: Occurs after OIR under bi-directional traffic.

  Workaround: Remove the service-policy in both affected device and peer and then re-attach to update counters.

- CSCsz47619

  Symptoms: ES-20 line card repeatedly resets.

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

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

- CSCsz47926

  Symptoms: An Error message that includes "IXP-MAP-QOS" is displayed on the supervisor. Occurs when an Ethernet flow point (EFP) interface is recreated or deleted and when online insertion and removal (OIR) is performed on a SPA with an EFP interface on SIP-400.

  Conditions: Occurs only when there is a EFP policy on a Gig V2 SPA on SIP-400.

  Workaround: There is no workaround. The issue does not impact functionality.

- 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.

- CSCsz52815

  Symptoms: If number of hours for statistics is increased to 10 or more after the probe is initially run and then restarted, system crashes with memory corruption

  Conditions: Occurs when the probe is started with the hours of statistics less than 10 and then re-started with the hours of statistics greater than 9.

  Workaround: There is no workaround.

- CSCsz53177

  Symptoms: When running Network Load-balancing (IGMP-mode) in VLANs with PIM enabled and static ARP entries for unicast IP to layer-2 multicast address, packet duplication will occur.

  Conditions: This symptom occurs when sending unicast (non-multicast) IP packets with multicast layer-2 destinations.

  Workaround: Use non-IGMP NLB modes (unicast or multicast with static macs) or use IGMP snooping querier instead of PIM on NLB SVIs.

- CSCsz54749

  Symptoms: Router crashes.

  Conditions: Occurs when configured with BGP damping and default IPv4 unicast address-family is deleted.

  Workaround: Do not delete the default IPv4 unicast address-family.

- 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.

- CSCsz58461

  Symptoms: Configuring **no negotiation auto** on Gigabit interface of 2xGEv2 SPA reduces duplex on interface to half. This causes traffic drop if traffic is bi-directional.

  Conditions: Occurs when "media-type" configured on Giginterface as "SFP".

  Workaround: There is no workaround.

- CSCsz59914

  Symptoms: When the SAMI module is booted up, CEF is disabled by default in the PPCs. If a PPC is configured for ISG, no static IP sessions (L2-connected or L3-routed) can come up. Even after enabling CEF, static IP sessions still do not come up. If the PPC(s) or SAMI gets reloaded after enabling CEF and writing the configurations into memory, sessions will come up.

  Conditions: When installing/configuring a new SAMI card for ISG, static IP sessions will not come up if CEF was disabled on bootup.

Workaround: Since the issue happens only when CEF was disabled on bootup, enabling CEF, doing a **write memory**, and then reloading the PPC will avoid this issue.

- CSCsz61156

  Symptoms: Routes do not appear in Routing Information Base (RIB) of a VRF.

  Conditions: Occurs with the following configuration:

  - Customer has IPv6 static route in VRF X.

  - Customer has configured BGP to import routes from VRF X into VRF Y.

  - BGP is apparently importing the VRF X route into VRF Y as requested

  - the routes are not showing up in VRF Y RIB

  Workaround: There is no workaround.

- CSCsz62046

  Symptoms: CPUHOG occurs in SNMP ENGINE, immediately followed by a crash.

  %SYS-3-CPUHOG: Task is running for (4000)msecs, more than (2000)msecs (91/87),process = SNMP ENGINE.

  Conditions: Querying cc6kxbarModuleChannelTable and cc6kxbarStatisticsTable in CISCO-CAT6K-CROSSBAR-MIB with invalid channel index may trigger this problem. The valid channel index range for the cc6kxbarModuleChannelTable and cc6kxbarStatisticsTable are (0..1)

  Regular snmp mibwalk on those 2 tables will not cause this problem.

  Workaround: Avoid MIB querying on cc6kxbarModuleChannelTable and cc6kxbarStatisticsTable with any specific invalid channel index. Instead just do regular SNMP MIBwalk on cc6kxbarModuleChannelTable and cc6kxbarStatisticsTable should be safe and work fine.

- CSCsz62528

  Symptoms: When configuring ATM or ima-group under controller T1/E1, the SNMP MIB does not populate the corresponding ATM interface. Because of this defect, ANA application is unable to model it correctly.

  Conditions: Problem exists on Cisco 7600 running Cisco IOS Release 12.2(33)SRC.

  Workaround: There is no workaround.

- CSCsz62974

  Symptoms: Router crashes while querying for cvpdnTemplateActiveSessions.

  Conditions: Occurs if the vpdn-template name is long.

  Workaround: There is no workaround.

- CSCsz63870

  Symptoms: On configuring HDLCoMPLS on SPA-8XCHT1/E1 SPA with 7600-SIP-400. traffic stops flowing from that interface.

  Conditions: Occurs when Xconnect is configured.

  Workaround: There is no workaround.

- CSCsz69988

  Symptoms: Connectivity Fault Management (CFM) packets are not transparently passed through scalable EoMPLS setup with SIP400 on the access side.

  Conditions: This happens when CFM is disabled after enabling it

Workaround: Perform an online insertion and removal (OIR) on the line card.

- CSCsz71782

  Symptoms: ASR crashes and reboots when RSIM sends VSA 1 command with wrong format.

  Conditions: VSA 1 format string has a colon which should not be there.

  vsa cisco generic 1 string "qos-policy-out:=remove-class(sub, (class-default, voip))"

  Workaround: There is no workaround.

- CSCsz72581

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

  Conditions: Occurs when using on-demand DPD.

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

- CSCsz73470

  Symptoms: When there are more than 8000 DHCP sessions on a Cisco 7600 ISG, a few dangling sessions are sometimes observed.

  Conditions: This symptom occurs when there are more than 8000 DHCP sessions on a Cisco 7600 ISG. ISG is configured as a DHCP relay.

  Workaround: Clear the sessions using the **clear ip subscriber dangling** command.

- CSCsz75715

  Symptoms: Policy-maps configured with random detect can cause unnecessary packet drops.

  Conditions: When an output policy-map is applied on SIP400 on Cisco IOS Release 12.2(33)SRD, and if class-maps are configured with "random detect", drops may occur even if the traffic is lower than the configured bandwidth percentage. If "random detect" is removed, drops is no longer seen. Also, this issue is seen only with low-speed interfaces. In this particular customer case, Gigabit Ethernet interface was configured in FastEthernet mode (speed 100mbps)

  Workaround: There is no workaround.

- CSCsz76701

  Symptoms: Sup720 crashes during ISIS adjacency flapping.

  Conditions: When an ISIS adjacency is flapping, issuing the command **show isis topology** triggered the crash. However, this observed only once in customer network

  Workaround: There is no workaround.

- CSCsz79094

  Symptoms: Router fails on a forced switchover to the standby supervisor card. The standby supervisor card tries to come online but encounters a crash and goes into ROMMon. To recover from this state the router requires a power cycle.

  Conditions: Occurs on Cisco 7600s running Cisco IOS Release 12.2(33)SRD2 and SRD2a and using non-Cisco SFPs.

  Workaround: Avoid non-Cisco SFPs or use a different release of Cisco IOS.

- CSCsz81473

  Symptoms: Subscriber upstream traffic stops flowing after an online insertion and removal (OIR) is performed on a line card, or when a pair of **shut/no shut** commands is entered when IP sessions are brought up on main interface. For ES+ line cards, the problem can be seen even for Port-Channel main interface and all non-access sub-interfaces.

Conditions: This defect is seen only when the main interface fails to get the same hidden VLAN allocated to it prior to line card OIR (or while entering **shut/no shut** commands).

Workaround: There is no workaround.

- CSCsz82587

  Symptoms: MPLS-TE configuration leads to router crash due to online insertion and removal (OIR).

  Conditions: MPLS-TE sessions coming up/down during OIR may lead to router crash.

  Workaround: There is no workaround.

- CSCsz82825

  Symptoms: When relaying to multiple servers, from an unnumbered interface, the Cisco IOS DHCP relay sends packets to all servers, even for packets where the client in a RENEWING state unicasting to attempt to reach a single server.

  ARP entries are retained for all OFFERed addresses, even if the client ultimately is using a different address. These extra ARP entries persist for several hours.

  Conditions:

  1. When relaying a DHCP packet on an unnumbered interface, and the DHCP client is in a renewing state (as determined by the fact), send it to the DHCP server that allocated the address so that we do not end up giving the client a new address, which would then interrupt the user sessions.

  2. When the client is in any other state, or if we do not get a response from the DHCP server, send to all helper-addresses.

  Workaround: There is no workaround.

  Further Problem Description: Only retain an ARP entry for the address that the DHCP client acknowledges. Do not retain addresses offered by DHCP servers that the client did not use in the ARP table.

- CSCsz89319

  Symptoms: Free memory is going down because SSS Manager is growing.

  Conditions: This symptom is observed on a Cisco 7600 that is used for ISG and that is running Cisco IOS Release 12.2(33)SRC3 under high network activity.

  Workaround: There is no workaround. Reload the router to free memory.

  Further Problem Description: The speed of the memory leak depends on the network activity. The more stress on the router, the faster the leak.

- CSCsz92345

  Symptoms: Unit under test crashes under heavy traffic when online insertion and removal (OIR) is performed on a SIP400.

  Condition: Occurs with huge Layer 2 and Layer 3 protocol configuration and SIP400.

  Workaround: There is no workaround.

- 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.

- CSCsz97011

  Symptoms: No Layer 4 Redirect (L4R) traffic is reaching the portal.

Conditions: Occurs if there is a sub-interface on the port facing the portal.

Workaround: There is no workaround.

- CSCsz97091

  Symptoms: Packet drop occurs when **show version**, **show run**, and **write memory** commands are issued.

  Conditions: Packet drop will be observed as input errors accounted as overruns. The rate of packets being dropped will be proportional to the rate of traffic.

  Workaround: There is no workaround.

- CSCsz99027

  Symptoms: Router crashes on applying/removing priority from service map.

  Conditions:

  1. Configure priority in class default. Apply it on EVC on ES20 line card.

  2. Remove priority from class default.

  3. Now, either removing or applying priority causes the router to crash.

  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" !

- CSCta04550

  Symptoms: Active supervisor may crash if standby supervisor resets for any reason.

  Conditions: This can happen if a interface level event happens around the same time of standby supervisor reload. The timing window is extremely small for the bug to happen.

  Workaround: There is no workaround.

- CSCta08632

  Symptoms: After supervisor forces switchover several times, a router two hops away has wrong ISIS topology and ISIS routing table.

  Conditions:

  1. Incremental shortest path first (ISPF) enabled in ISIS.

  2. **set-overload-bit** on-startup in ISIS.

  3. Supervisor force switchover several times

  Workaround: Disable ISPF in ISIS.

- CSCta10442

  Symptoms: Policy-map not applied at SIP400 in dLFI over ATM case after performing **shut/no shut** of the interface.

Conditions: Occurs after performing **shut/no shut** on the interface.

Workaround: Perform an online insertion and removal (OIR) on the SIP400.

- CSCta10908

  Symptoms: We will see the traffic loss when there is a cut-over in the Spatial Reuse Protocol (SRP) ring.

  Conditions: There should be HWEoMPLS configured in the system. Ingress card should be DFC card (not a supervisor card), and core-facing card should be SRP card.

  Workaround: Either we use the supervisor card as ingress card, or we need to write to EARL adjacency on the line card using the **test mls cef adjacency** command.

- CSCta15786

  Symptoms: Polcy-based routing (PBR) stops working after stateful switchover (SSO). All traffic that should be policy-routed is dropped instead.

  Conditions: This usually happen after several switchovers between supervisors. Usually problem occurs after about 10 switchovers, however, it could happen after first one.

  Workaround: Remove and add policy on the interface.

- CSCta20257

  Symptoms: BGP modifies next-hop of the route owned by other protocol in Routing Information Base (RIB).

  Conditions: Occurs when other protocol route is best in RIB due to lower admin distance, and BGP trys to add the route to RIB.

  Workaround: Enter the **clear ip route***x.x.x.x* command.

- CSCta25363

  Symptoms: The **show mls qos module** command is not relevant for ES+ line cards and produces invalid output.

  Conditions: Occurs during normal operation.

  Workaround: Do not use the **show mls qos module** for ES+ line cards.

- CSCta26029

  Symptoms: Path attribute memory leak is found when there is some path attribute churn in the network.

  Conditions: The symptom is seen only when there are idle peers on the router.

  Workaround: Unconfigure the idle peers.

- CSCta26071

  Symptoms: A Cisco IOS platform can crash when authorizing Radius profiles. The issue is due to an invalid terminal sync change that updated the incorrect enumeration structure, leading to one enumeration having 1 too many entries and another one too few.

  When parsing the "protocol" or "service" field, the AAA code may walk beyond the boundaries of a string array associated with the above mentioned enumerations. This will cause platforms such as the Cisco ASR to crash.

  Conditions: This crash has been observed on a Cisco ASR1004 (RP2) that is running the Cisco IOS-XE version Cisco IOS Release 12.2(33)XNC1t.

Workaround: This crash will occur if an invalid protocol or service field is provisioned in a Cisco VSA. However, even when valid protocols or services are used, it is possible that certain enumeration walking code may also trigger a crash. However, Cisco has not been able to validate that situation. As a consequence, when using branches such as Cisco IOS Release 12.2(33)SB or Release 12.2XNC, without this fix, it is critical that no invalid Cisco VSA be used.

- CSCta30344

  Symptoms: Relay information option is not verified in the downstream DHCP packets.

  Conditions: This happens only when option 82 insertion is configured at the interface configuration mode.

  Workaround: Configure option 82 in global configuration mode.

- CSCta34908

  Symptoms: Following error message is displayed:

  SPA_EEPROM-3-RPC_FAILED: Failed to send RPC message to read EEPROM of SPA in subslot 7/0 - rpc timeout error after fpd upgrade.

  Conditions: This error usually seen following reload of the SPA after FPD upgade of SPA.

  Workaround: Perform an online insertion and removal (OIR) of SPA. If that does not work, then reload line card.

- CSCta42753

  Symptoms: Following reload or reseat of Protect LC in ADM TRuepointR 6400, SPA-2OC3-POS/SIP400/SRD2 reports "Received Alarm: L-AIS" on the PROTECT port of a 1+1 APS group when an inline SONET analyzer attached to same wire reports no L-AIS is present on the wire.

  Conditions: L-AIS is recovered by an STE via looking for K2 = 0x07 for 5 consecutive frames.

  A Cisco POS interface with "pos ais-shut" will transmit L-AIS when interface is shutdown. Without "pos ais-shut" the interface continues to send valid SONET frames toward the STE/LTE.

  Workaround: Remove/reinsert the cable on CPE to clear the alarm.

- CSCta43713

  Symptoms: Port-channel on interface of ES+, a line card reload causes memory leak on "RPC pagp_switch_sp2mp" and "QM_VLOU_MAP". It loses about 748 bytes per policy-map attached on interface.

  Conditions: Occurs on a Cisco 7600 series router with policy-map configured on port channel interface.

  Workaround: There is no workaround.

- CSCta46650

  Symptoms: The console gets stuck when the **show arp** command is executed and "esc" is pressed to stop viewing the whole output.

  Conditions: The symptom is observed with 512 ARP sessions on the system and set term len equal to 20.

  Workaround: There is no workaround.

- CSCta46653

  Symptoms: In ES+ line cards with link daughter card versions less than .200, there is a possibility of the line card crash when an SFP module is removed and inserted.

  Conditions: Occurs under normal operating conditions.

Workaround: There is no workaround.

- CSCta58194

  Symptoms: Router crashes with max-entries of NAT translations limit imposed.

  Conditions: With **ip nat max-entries limit <>** configured and greater than limit number of flows passed through the NAT router, crash is seen when the above limit configuration is removed and a large amount of translations are created.

  Workaround: There is no workaround.

- CSCta61663

  Symptoms: Cisco 7600 SPA-1XCHSTM1/OC3 SPA does not use the configuredn etwork-clock source as the reference for the T1/E1.

  Conditions: The SPA-1XCHSTM1/OC3 SPA is configured to use the internal clock for timing of the T1/E1. The network-clock is configured on the Cisco 7600 to use the reference from an ATM OC3 interface.

  Workaround: There is no workaround.

- CSCta65610

  Symptoms: When configuring an OSPF sham-link between two PEs also used for multicast VPN, RPF check for the source of a multicast stream points to the physical interface used by the sham-link instead of the tunnel.

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

  Workaround: There is no workaround. Prefixes must be learned through i-BGP.

- CSCta68856

  Symptoms: Policy map with multiple MAC ACL filters matches only the traffic with the first MAC ACE in the ACL.

  Conditions: Occurs on a Cisco 7600 series router with ES+ linecard, and with policy map with MAC ACL configured on ES+ linecard interface.

  Workaround: There is no workaround.

- CSCta69232

  Symptoms: Resilient Ethernet Protocol (REP) will not converge if REP is configured over switchport and **vlan dot1q tag native** is enabled.

  Conditions: In this case, the REP PDUs will be sent as tagged packets.

  Workaround: There is no workaround.

- CSCta77105

  Symptoms: Hierarchical service policy is not attached to multilink on SIP-200

  Conditions: When the hierarchical service-policy is applied on the interface on sip1 or sip2, it is rejected.

  Workaround: There is no workaround.

- CSCta77747

  Symptoms: If a ES+ port is configured as switchport trunk and the Cisco 7600 is supposed to route the traffic between the vlans carried in the trunk, routing is not happening.

  Conditions: Occurs when ES+ ports are configured as switchports, such as follows:

interface GigabitEthernet2/2

switchport

switchport trunk allowed vlan 666,777

switchport mode trunk

Workaround: Use EVC instead of switchport, such as follows:

interface GigabitEthernet2/2

no switch

service instance 10 ethernet

encapsulation dot1q 666

rewrite ingress tag pop 1 symmetric

bridge-domain 666

!

service instance 20 ethernet

encapsulation dot1q 777

rewrite ingress tag pop 1 symmetric

bridge-domain 777

- CSCta78252

  Symptoms: If the link flaps on a multilink bundle, or if the CE router is hard reset, when the bundle comes back up, it will not pass traffic until all but one of the interfaces of the bundle are removed.

  Conditions: Occurs on a router running Cisco IOS Release 12.2(33)SRD2.

  Workaround: There is no workaround.

- CSCta79634

  Symptoms: System crash in L2TP. Following this, most of the L2TP setups fail.

  Conditions: The symptom occurs at an L2TP control-plane event.

  Workaround: Clear VPDN again or reload the router.

- CSCta89002

  Symptoms: Following error message is displayed:

  EARL_L2_ASIC-SP-4-L2L3_SEQ_ERR, EARL L2 ASIC #0: L2L3 Mismatch seq #0x507 and %CPU_INTF_FPGA-5-PAUSE_FAIL

  After this message, router crashes.

  Conditions: Occurs when sending large a amount of IPv4 packets towards FlexWAN2 with bad version in short span, such as >1000pkts at line rate.

  Workaround: There is no workaround.

- CSCta91367

  Symptoms: Bus error crash on SIP-600 SPA-10X1GE-V2.

  Conditions: Crash is specific to SIP-600 when a applying QinQ configuration to the sub-interface of a GE.

  Example:

  interface GigabitEthernet1/0/0.1

encapsulation dot1Q XXX second-dot1Q XXX

Thus far, this has been seen on Cisco IOS versions based on 12.2(33)SRB and 12.2(33)SRD.

Workaround: Have verified that the SIP-400 with SPA-2X1GE and 7600-ES20-GE3CXL support QinQ with Cisco IOS Release 12.2(33)SRB3.

- CSCta99162

  Symptoms: When the command **passive-interface default** is entered under router ISIS, the router reloads.

  Conditions: Enter router ISIS configuration mode and enter the **passive-interface default** command. Router reloads.

  Workaround: Configure a passive interface under router ISIS.

- CSCtb05885

  Symptoms: CEM circuit on Cisco 7600 CEoP SPA does not forward AIS alarm towards attachment circuit even though it is in "TDM Fault" condition as indicated by the output of **show cem circuit detail**. It also incorrectly shows the CEM circuit as being in "Packet loss" state.

  Conditions: This happens only when CEM circuit is in "TDM Fault" condition.

  Workaround: There is no workaround.

- CSCtb08593

  Symptoms: ES40 crashes continuously and powers down.

  Conditions: Occurs when configuring default native VLAN on a subinterface with dot1q encapsulation.

  Workaround: Remove the dot1q encapsulation configuration.

- CSCtb22873

  Symptoms: If **show mpls forwarding with owner***owner* command is issued in cases where none of the entries in a very large forwarding table match the specified owner, a CPUHOG error and traceback may occur.

  Conditions: This problem would only occur in cases where a configuration generating a very large MPLS forwarding table existed.

  Workaround: Do not issue this command for an owner that did not create any labels.

- CSCtb33667

  Symptoms: Serial interface in CH0C3 SPA in mode CT3 does not come up. SONET controller and the T3 controller are up, but T1 controller that is configured under T3 is down with LOF alarm.

  Conditions: Occurs when configuring STS-1 in CT3 or CT3-E1 mode.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRD2a

Cisco IOS Release 12.2(33)SRD2a is a rebuild release for Cisco IOS Release 12.2(33)SRD. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRD2a but may be open in previous Cisco IOS releases.

- CSCsv79583

Symptoms: When coarse wavelength division multiplexing (CWDM) small form-factor pluggable (SFP) module of any wave length is inserted in the GE port or OC48 port, the SFP module is disabled and the following message is displayed:

```
%TRANSCEIVER-3-NOT_COMPATIBLE: SIP0/0: Detected for transceiver module in
GigabitEthernet0/0/0, module disabled
```

The output of the **show status** command shows the following:

```
CE1#show hw-module subslot 3/3 transceiver 1 status
The transceiver in slot 3 subslot 3 port 1 has been disabled because: the transceiver
type is not compatible with the SPA.
```

Conditions: This issue is seen with a new version of CWDM SFP in which the EEPROM programming has been changed. All releases prior to Cisco IOS Release 12.2(33)SRE and 12.2(33)SRD3 are incompatible with the new SFP version. For the Cisco ASR 1000, all software releases prior to 12.2(33)XNC release 3 and release 4 are affected.

Workaround: Issue is not seen with the older version of SFP.

- CSCta46653

  Symptoms: In ES+ line cards with link daughter card versions less than .200, there is a possibility of the line card crash when an SFP module is removed and inserted.

  Conditions: Occurs under normal operating conditions.

  Workaround: There is no workaround.

Resolved Caveats—Cisco IOS Release 12.2(33)SRD2

Cisco IOS Release 12.2(33)SRD2 is a rebuild release for Cisco IOS Release 12.2(33)SRD. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRD2 but may be open in previous Cisco IOS releases.

- CSCdy26008

  Symptoms: The negotiated IP address is not cleared from an asynchronous interface when a call ends, even though the IP address is returned properly to the IP peer pool.

  Conditions: This symptom is observed when the peer is configured to dial in to the network access server (NAS) and to obtain an IP address through IP Control Protocol (IPCP) negotiations with the NAS. The NAS is configured with pools of IP addresses to be allocated to the peer when the peers generate a PPP call to the NAS. The NAS is also configured to authenticate the peer through RADIUS.

  Workaround: There is no workaround.

- CSCec72958

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

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

  Workaround: There is no workaround.

- CSCec85585

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

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

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

- CSCeg80842

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

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

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

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

- 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**.

- CSCek75694

  Symptoms: A router running Cisco IOS 12.4T may reload unexpectedly

  Conditions: Occurs when BFD is configured and active.

  Workaround: Disable the BFD feature.

- CSCin01217

  Symptoms: A router may not allow the peak cell rate value on an interface that is bundled with more than one ATM T1 interface or more than one ATM E1 interface to be set to a value that is more than the bandwidth of one T1 ATM interface or one E1 ATM interface.

  Conditions: Occurs on Cisco 3600 routers Cisco IOS Release 12.2(6.8)T2

  Workaround: There is no workaround.

- CSCin91677

  Symptoms: The Unavailable Seconds (UAS) that are displayed in the output of the **show controllers serial** *slot/port* command are incorrect. The display of the UAS starts only after 20 contiguous severely errored seconds (SES) instead of after 10 contiguous SES.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with a PA-T3+ port adapter.

  Workaround: There is no workaround.

- CSCsb61514

  Symptoms: Packets larger than 1526 bytes get dropped between supervisor and Cisco Multi-Processor WAN Application Module (MWAM) on a Cisco 7600.

  Conditions: Drops were seen even after increasing MTU size.

Workaround: Reduce MTU on tunnel end systems, which increases fragmentation.

Further Problem Description: The problem is reproducible with extended pings of size 1527 bytes, which get dropped in direction SUP->MWAM as diagnosed with **deb ip icmp**.

- CSCsb98906

  Symptoms: A memory leak may occur in the "BGP Router" process.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(26)S6, that is configured for BGP, and that has the **bgp regexp deterministic** command enabled.

  Workaround: Disable the **bgp regexp deterministic** command.

- CSCsc78999

  Symptoms: An Address Error exception occurs after Uninitialized timer in TPLUS process.

  Conditions: This is a platform independent (AAA) issue. It may be seen with a large number of sessions while accounting is configured with a T+ server.

  Workaround: Disable accounting, or use RADIUS accounting instead of a T+ server.

- CSCse29570

  Symptoms: Router might unexpectedly reload during CNS configuration download.

  Conditions: The downloaded configuration must disable the CNS configuration initial or partial for this crash to occur.

  Workaround: Use static configuration and prevent configuration download from CNS server.

- CSCse87210

  Symptoms: On Catalyst 6500 Series and Cisco 7600 Series, when certain service modules transmit packets to VLANs also used with Distributed EtherChannel (DEC), those packets may be dropped and lost. For further description, please review "Field Notice: FN-61935 - Catalyst 6500 Series and 7600 Series Service Module Incompatibility With Distributed EtherChannel and Packet Re-Circulation."

  Conditions: The problem only happens when service cards are operating in crossbar-enabled mode.

  Workaround: See the above referenced Field Note for several workarounds.

- CSCse97209

  Symptoms: Standard communities are not set correctly by an outbound route-map.

  Conditions: Occurs when route-map uses *continue* option.

  Workaround: There is no workaround.

- CSCsf25157

  Symptoms: An IPv6 ping may fail when the **atm route-bridged ipv6** command is enabled.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.3(22.13), interim Release 12.4(13.9), or Release 12.4(13b) and that is configured for QoS.

  Workaround: There is no workaround.

- CSCsg11616

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

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

  Workaround: There is no workaround.

- CSCsg39754

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

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

  Workaround: There is no workaround.

- CSCsh48947

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

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

  Workaround: There is no workaround.

- CSCsi88974

  Symptoms: While configuring a mediation device (MD), if the MediationSrcInterface is set to loopback interface, traffic will cause MALLOC failures.

  Conditions: Problem is seen when traffic rate is equal to or greater than 8000 packets per second.

  Workaround: Do not use loopback0 as MD source interface.

- CSCsj34557

  Symptoms: Router displays following error message and reloads:

  Jun 18 06:12:23.008: event flooding: code 10 arg0 0 arg1 0 arg2 0

  ```
  %SYS-3-OVERRUN: Block overrun at E5D8310 (red zone 00000000) -Traceback= 0x6080CEB0
  0x60982108 0x60982EC0 0x6098511C 0x609853BC %SYS-6-MTRACE: mallocfree: addr, pc
  662B5B1C,608A6F3C 0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6 662B5B1C,608A6F3C
  0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6 %SYS-6-MTRACE: mallocfree: addr, pc
  662B5B1C,608A6F3C 0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6 662B5B1C,608A6F3C
  0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6 %SYS-6-BLKINFO: Corrupted redzone blk
  E5D8310, words 6088, alloc 61FE2638, InUse, dealloc 80000000, rfcnt 1 -Traceback=
  0x6080CEB0 0x609681D4 0x6098211C 0x60982EC0 0x6098511C 0x609853BC %SYS-6-MEMDUMP:
  0xE5D8310: 0xAB1234CD 0xFFFE0000 0x0 0x63894208 %SYS-6-MEMDUMP: 0xE5D8320: 0x61FE2638
  0xE5DB2D0 0xE5D8144 0x800017C8 %SYS-6-MEMDUMP: 0xE5D8330: 0x1 0x0 0x1 0x64B53478
  ```
  %Software-forced reload

  Conditions: Occurred on a Cisco 7200 running the c7200-ik9s-mz.124-7a.bin image.

  Workaround: There is no workaround.

- CSCsj78403

  Symptoms: A router may crash when the **clear ip bgp** command is entered.

  Conditions: Occurs on devices running BGP and configured as a route reflector client with conditional route injection configured.

  Workaround: Unconfigure conditional route injection.

- CSCsk04318

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

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

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

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

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

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

- CSCsk49705

  Symptoms: The **ip nat inside source static network** command does not have the <cr> option.

  Conditions: This symptom is observed on a Cisco 7200 router that is loaded with Cisco IOS Release 12.4 or 12.4T.

  Workaround: There is no workaround.

- CSCsk94179

  Symptom: Connectivity problems are observed for IPv6 client, which obtained IPv6 prefix via DHCP for Virtual Access interface, due to incorrect static routes in the routing table for the assigned IPv6 prefix.

  Conditions: Occurs with IPv6 prefix delegation via DHCP, when client moves from one interface to another.

  Workaround: None

  Further problem description: When IPv6 prefix delegation assigns a prefix for Virtual Access interface, it creates a static route for the prefix in the routing table. When a client moves to a new interface, old binding and the old routes are retained, which causes the problem.

- CSCsl00472

  Symptoms: A Cisco router unexpectedly reloads with memory corruption after showing multiple "%SYS-2-INPUT_GETBUF: Bad getbuffer" messages

  Conditions: Occurs during normal operation.

  Workaround: There is no workaround.

- CSCsl04687

  Symptoms: "Total packets L3 Switched" counter does not include multicast packet count.

  Conditions: Occurs always. "Total packets L3 Switched", includes packet switched by FIB, NetFlow and ACL only.

  Workaround: There is no workaround.

- CSCsl32142

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

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

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

- CSCsl68327

  Symptoms: Packets may be lost during rekey.

  Conditions: Occurs because IPSec transit packets may trigger invalid SPI.

  Workaround: There is no workaround.

- CSCsl71704

  Symptoms: A receive access control list (rACL) with large ACL is not applied on interface if is QoS configured.

  Conditions: Occurs when rACL with large ACL is applied on an interface. It consumes over 60% of ternary content addressable memory (TCAM) space. If the rACL is applied a second interface with QoS, the configuration fails without displaying an error message.

  Workaround: There is no workaround.

- CSCsm28287

  Symptoms: After shutting down a GRE tunnel interface, the active RP crashed and switchover took place. The following error message was displayed:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address 13:02:45 UTC Fri Jan 18 2008 addr=0xD,
  pc=0x7144A5A0, ra=0x7209FFF8, sp=0x5ABEE90 SLOT0:01:40:03: %DUMPER-3-PROCINFO: pid =
  16409: (sbin/ios-base), terminated due to signal SIGBUS, Bus error (Invalid address
  alignment) SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: zero at v0 v1
  SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: R0 00000000 7A5FD854 EF4321F9
  7A6452D0 SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: a0 a1 a2 a3 SLOT0:01:40:03:
  %DUMPER-3-REGISTERS_INFO: 16409: R4 EF4321CD 0000000B 0000000B 00000000
  SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: t0 t1 t2 t3 SLOT0:01:40:03:
  %DUMPER-3-REGISTERS_INFO: 16409: R8 7CB96E10 00FDDBE0 00000000 EFFFFFFF
  SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: t4 t5 t6 t7 SLOT0:01:40:03:
  %DUMPER-3-REGISTERS_INFO: 16409: R12 00000000 F7E8E12F 00000000 00000000
  SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: s0
  ```

  Conditions: Occurred on a Cisco 7200 running an internal build of Cisco IOS Release 12.2SX.

  Workaround: There is no workaround.

- CSCsm47417

  Symptoms: W2:setting ceExtSysBootImageList cause **write memory** to work incorrectly.

  Conditions: Occurs after setting ceExtSysBootImageList to a new boot image from SNMP. The new boot image in running-config is not copied to startup-config. Instead, a variable “d” will be copied to startup-config after the **write memory**. The **show bootvar** command will show BOOT variable = d.

  ```
  Example: bgl11-lab1-tftp1:/auto/sw/packages/snmpr/15.1.0.3/solaris2bin:3>
  bgl11-lab1-tftp1:/auto/sw/packages/snmpr/15.1.0.3/solaris2bin:3>getmany -v2c
  10.64.68.138 public ceExtSysBootImageList ceExtSysBootImageList.2001 =
  disk1:s72033-adventerprisek9_dbg-vzsm47417test ceExtSysBootImageList.2017 =
  disk1:s72033-adventerprisek9_dbg-vzsm47417test
  bgl11-lab1-tftp1:/auto/sw/packages/snmpr/15.1.0.3/solaris2bin:4>setany -v2c
  10.64.68.138 public ceExtSysBootImageList.2001 -o "disk1:" ceExtSysBootImageList.2001
  = disk1: ---------------------------------------------- 7600-11-1# 00:02:56:
  %SYS-5-CONFIG_I: Configured from 10.64.71.240 by snmp
  ```

Workaround: There is no workaround.

- CSCsm53196

  Symptoms: Crash occurs at “ip_route_delete_common”.

  Conditions: Occurs under the following scenario:

  1)A multicast BGP route exists.

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

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

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

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

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

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

- CSCsm55817

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

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

  Workaround: Do not use handles that start with “00”.

- 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.

- CSCsm71537

  Symptoms: The router crashes when Independent Optimized Edge Routing (OER) is configured.

  Conditions: Occurs when OER is configured.

  Workaround: There is no workaround.

- CSCsm86832

  Symptoms: The line protocol of the serial interface keeps flapping.

  Conditions: This symptom is observed after the Atlas BERT pattern is run on a fractional T1 (1 or 2 timeslots).

  Workaround: Add/Remove the T1.

- CSCso00864

  Symptoms: System running in **crypto engine mode vrf** with SVI interfaces that have crypto map attached and is in SSO redundancy mode may experience crash of the standby supervisor when the interface referenced by **crypto map local address** is modified.

  Conditions: The system is in SSO redundancy mode, has SVI interfaces with crypto map configuration and running in “VRF mode”.

Workaround: There is no workaround.

- CSCso29361

  Symptoms: The commands given in the **interface range** command may not be synced to all interfaces configured in the range in the standby supervisor.

  Conditions: Occurs when configuration commands are entered under **interface vlan range** command. They get attached to only the first VLAN in the range in the redundant supervisor. After switchover, traffic does not flow due to the missing VLAN configuration.

  Workaround: There is no workaround.

- CSCso42170

  Symptoms: CPUHOG and traceback messages seen for IP NAT ager process.

  Conditions: Occurs when NAT is configured with dynamic translations greater than 27,000, and the NAT pool is exhausted. The following messages are seen:

  ```
  05:13:43: %SYS-3-CPUHOG: Task is running for (2000)msecs, more than (2000)msecs
  (19/13),process = IP NAT Ager. -Traceback= 40BA0994 40BA0F00 40B983A8 40B9852C
  413C2B08 413C2AF4
  ```

  Workaround: There is no workaround.

- CSCso56038

  Symptoms: The following error message may be seen:

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

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

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

  Workaround: There is no workaround.

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

- CSCso57020

  Symptoms: Etherchannel states for Link Aggregate Control Protocol (LACP) port-channels are inconsistent between active and standby, which could possibly affect traffic forwarding.

  Conditions: Occurs while configuring several LACP port channels. This could be seen if LACP port channels are configured and the device is brought up in SSO mode.

  Workaround: Once the standby is completely up in HOT state, perform a **shut/no shut** on the interfaces that are inconsistent.

- CSCso65266

  Symptoms: A customer upgraded to Cisco IOS Release 12.0(32)Sy4, and now the customer is seeing a memory leak in the BGP process. The memory leak is happening with the BGP router process at the rcach chunk memory when the route map has a “continue” clause in the configuration.

  Conditions: The leak is seen when a “continue” statement is configured in a inbound/outbound route map.

  Workaround: There is no workaround.

- CSCso74922

  Symptoms: Resilient Ethernet Protocol (REP) state flaps after line card reset

  Conditions: Occurs on routers running Cisco IOS Release 12.2(33)SRD with SIP600 ports configured as REP edge ports.

  Workaround: There is no workaround.

- CSCso84567

  Symptoms: Non-TCP traffic passing through the device is punted to the control plane policer. When Control Plane Policing (CoPP) is configured, the bridge result is changing to policy route because WCCP is being applied to all IP packets of a WCCP service.

  Conditions: Both WCCP and CoPP must be enabled for this issue to occur.

  Workaround: There is no workaround.

- CSCso88138

  Symptoms: When there is a link flap or a reload, RSVP shows that the interface is down while actually the interface is up. Because of this, the tunnel may take a backup path even when the interface is up.

  Conditions: Unknown at this time.

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

- CSCso90058

  Symptoms: MSFC crashes with Red Zone memory corruption.

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

  Workaround: There is no workaround.

- CSCso90970

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

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

  Workaround: There is no workaround.

- CSCsq04355

  Symptoms: Customer mistakenly modified the service module SPAN session which caused high CPU on the switch. This caused the interface to flap, bringing down Hot Standby Routing Protocol (HSRP), Open Shortest Path First (OSPF) and other protocols resulting in an outage.

  Conditions: Occurs when manipulating the service module SPAN session

```
LAB1(config)#monitor sess 1 source vl 2028
% Session 1 used by service module
LAB1(config)#no monitor sess servicemodule
LAB1(config)#do sh mon
```
Session 2

```
---------

Type : Local Session
Source Ports :
Both : Gi2/2
Destination Ports : Gi3/2
LAB1(config)#monitor sess 1 source vl 2028
```

```
LAB1(config)#do sh mon
```
Session 1

```
---------
Type : Local Session
Source VLANs :
Both : 2028
Session 2
---------
Type : Local Session
Source Ports :
Both : Gi2/2
Destination Ports : Gi3/2
```
Workaround: Do not modify or change the SPAN session related to the service module using the session number. Instead use **no mon session servicemodule** in order to remove the session.

- CSCsq06208

  Symptoms: When health monitoring (HM) diagnostic failure happens, call-home diagnostic messages are not out before platform action is taken.

  Conditions: Call-home is subscribed to diagnostic alert group minor or major error and the gold policy is active. It only happens when the HM diagnostic test interval is small enough.

  Workaround: Set the HM diagnostic test interval to be large enough, but there is no guarantee it will work in all test cases.

  Further Problem Description: Because gold policy is last policy in EEM queue, it waits for call-home messages to send out before it executes. If gold policy continues to trigger on the next test failure after reaching the threshold when action notify flag is already false, it does not need to wait for call-home message to execute. It could crash the system before the call-home message for the last gold policy finishes.

  Adding ACTION_NOTIFY TRUE condition to the gold policy will prevent the gold policy to continuously execute and consistent with call-home message triggering condition.

- CSCsq14261

  Symptoms: Downstream traffic will drop when we send IPv6 traffic over PPPoE sessions.

  Conditions: Bring up a PPPoE session over L2TP tunnel for address negotiated by IPv6, then send downstream IPv6 traffic.

  Workaround: There is no workaround.

- CSCsq14311

  Symptoms: Router crashed while clearing NAT translations.

  Conditions: Occurred on a Cisco 7200.

  Workaround: There is no workaround.

- CSCsq37953

  Symptoms: Junk value is seen in stand-by router.

  Conditions: Junk value is observed in stand-by router when normal ATM PVC is created. After switch-over, junk value is seen in both active and stand-by routers.

  Workaround: There is no workaround.

- CSCsq39079

  Symptoms: During periods of high IKE initial session establishment the, SPA may crash.

  Conditions: Occurs with high number of simultaneous IKE sessions being established.

Workaround: There is no workaround.

- CSCsq42885

  Symptoms: Line card crashes recurrently with the “Address exception error”.

  Conditions: The issue is seen when entering the **no shutdown** command on the spatial reuse protocol (SRP) interface.

  Workaround: There is no workaround.

- CSCsq51378

  Symptoms: ATM PA Interface with no cables connected shows up/up after forced redundancy.

  Conditions: Occurred under the following scenario:

  - No cables attached to Fast Ethernet or ATM interface.

  - Issue **no shut** on interface.

  - The **show ip int brief** command shows interface status up/protocol down.

  - After **redundancy force** command is entered, interface shows up/up (no cables connected).

  This affects Fast Ethernet interfaces and ATM interfaces on WS-x6582-2PA/PA-2FE-TX and PA-A3-OC3-MM. It does not affect Supervisor ports or Serial Interfaces.

  Workaround: There is no workaround.

- CSCsq53542

  Symptoms: After stateful switchover (SSO) there may be loss of multicast packet delivery for 10 or more seconds.

  Conditions: Occurs when multicast routing is enabled in the default mode.

  Workaround: If there are no mStatic or mBGP routes, the following configuration will avoid the problem:

  ```
  Router(config)#ip multicast rpf multitopology Router(config)#global-address-family
  ipv4 multicast Router(config-af)#topology base Router(config-af-topology)#use unicast
  base Router(config-af-topology)#
  ```

- CSCsq55691

  Symptoms: QoS with Link Fragmentation and Interleaving (LFI) over ATM does not work.

  Conditions: Occurs after a **shut/no-shut** on the ATM interface

  Workaround: Reload the line card on both ends.

- CSCsq60016

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

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

  Workaround: Break the entry into shorter strings.

- CSCsq77282

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

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

  Workaround: There is no workaround.

- CSCsq77571

  Symptoms: Router (SP) crash may happen upon deleting multiple VRFs or unconfiguring multiple MDTs.

Conditions: The crash is seen when trying to delete multiple MDTs at one time.

Workaround: Allow at least seconds after each MDT delete command or VRF delete command before issuing the next command.

- CSCsr05746

  Symptoms: ESM20 line card may crash while booting up.

  Conditions: Occurs intermittently with a scaled topology.

  Workaround: There is no workaround.

- CSCsr09062

  Symptoms: Cisco 7200 crashes due to memory corruption.

  Conditions: Occurs when MLP+QoS is configured on a Cisco 7200 router. QoS policy is having bandwidth, change the BW parameter and flap the multilink using **clear int multilink1** to see the crash.

  Workaround: There is no workaround.

- CSCsr18589

  Symptoms: A Virtual Router Redundancy Protocol (VRRP) group configured on a VLAN interface flaps from the backup to the master state after stateful switchover (SSO) when the existing master is still available on the network. The group will flap back to backup a short period later.

  Conditions: The problem only occurs when there are a large number of VLAN interfaces with a VRRP group configured on each interface and SSO is performed.

  Workaround: Each of the VRRP groups can be configured with a larger VRRP advert timer value. Values should be varied depending on the setup, but a larger than default value is usually required.

- CSCsr18942

  Symptoms: Traceback occurs when VPN routing/forwarding (VRF) is deleted and then recreated.

  Conditions: Occurs when multicast RP is configured under VPN routing/forwarding (VRF) first. When the VRF is deleted, some multicast data may still be locked and not deleted, causing the traceback when a new VRF is created and multicast RP is configured there.

  Workaround: There is no workaround.

- CSCsr26025

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

  Conditions: Occurs under the following scenario:

  - Border Gateway Protocol (BGP) with two neighbors sending a default gateway. - Static route “0.0.0.0/8 to null 0" is configured. - Failover takes place and RIB is not updated.

  Workaround: There is no workaround.

- CSCsr27727

  Symptoms: A Cisco Catalyst 6000 reports the following message and unexpectedly reloads:

  %SYS-2-ASSERTION_FAILED: Assertion failed: “wccp_acl_item_valid(item,NULL)”

  Conditions: This symptom is observed on a WS-C6509 that is running Cisco IOS Release 12.2(33)SXH2a.

  A WCCP service is configured with a redirect-list referring to a simple ACL.

  Workaround: Use an extended ACL as the WCCP redirect-list.

- CSCsr29468

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

  Cisco has released free software updates that address this vulnerability.

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

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

- CSCsr41079

  Symptoms: Error message seen after stateful switchover (SSO):

  %CHKPT-4-NOMESSAGE: Message is NULL, (Cannot get data ptr)

  Conditions: Occurs when Intermediate System-to-Intermediate System (IS-IS) NSF is configured.

  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.

- CSCsr45502

  Symptoms: A router intermittently runs into crashes in a large scale network with active PPPoEoA sessions.

  Conditions: This symptom occurs when many active PPPoEoA sessions exist.

  Workaround: There is no workaround.

- CSCsr49316

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

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

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

- 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**.

- CSCsr53264

  Symptoms: A software-forced crash occurs on the RP of a Cisco 7600 running Cisco IOS Release 12.2(33)SRB2.

  Conditions: Occurs when the clear route-map counters <name> command is entered.

  Workaround: Upgrade to Cisco IOS Release 12.2(33)SRC3 or later.

- CSCsr54959

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

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

  Workaround: There is no workaround.

- CSCsr55713

  Symptoms: A crash occurs.

  Conditions: The crash is caused by a ping across an ISATAP tunnel. The symptom is observed only in Cisco IOS Release 12.4(15)T7 on the Cisco 7200 (it is not known to affect other platforms), since the crash is dependent on the Cisco IOS memory map (which varies with each image).

  Workaround: There is no workaround.

- CSCsr55922

  Symptoms: The EIGRP IPv6 process may incorrectly select a router-ID from the 127.0.0.0 address range.

  Symptoms: The same router-ID may be selected on two separate Cisco routers configured for EIGRP IPv6. External prefixes advertised by one of the EIGRPv6 routers will be ignored by the receiving EIGRPv6 router due to the fact the routerID contained in the external data portion of the prefix matches the receiving routerID; a loop prevention method.

  Workaround: Manually configure a router-ID under the EIGRP IPv6 process with **router-id**<*address*> command.

- CSCsr56465

  Symptoms: Line card MAC notification test fails when redundancy mode is changed from RPR to SSO or SSO to RPR. SIP-400 Bus Connectivity Test failed when the following commands are issued:

  Conf t redundancy mode rpr

  Conditions: The issue observed in the Fabric Hot Sync-enabled Sup720 and RSP720 routers Cisco IOS Release 12.2(33)SRC. In the problem state, Super Santa Ana (SSA) channels are out of sync. For example, **show platform hard ssa status** will display SSA channel status from the SSA based CWAN module console.

  Workaround: There is no workaround.

- CSCsr60252

  Symptoms: MPLS Layer 3 VPN with HQOS on PA-A6-OC3 with 500 ATM PVCs crashes at PEs wth online insertion and removal (OIR).

  Conditions: Perform a soft OIR of PE while entering the **hw-module slot 5 start** command to observe the crash.

  Workaround: Configure with HQoS for 500 PVCs.

- CSCsr60789

  Symptoms: Occasionally a crash occurs after preemptive switchover with no traffic.

  Conditions: Unknown. Issue is not reproducible on a consistent basis.

  Workaround: There is no workaround.

- CSCsr68497

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

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

Workaround: There is no workaround.

- CSCsr68528

  Symptoms: When there is heavy traffic on the 10-GE SPA (that is, 80 percent or more of line rate), and the interface is shut/no shut, there is a low probability that the interface may become stuck and incorrectly send pause frames on the connected link, interrupting traffic flow. This is also seen on ES20 line cards with 10-GE ports. (CSCsx82439)

  Conditions: This symptom is observed when the link is shut/no shut while there is a high level of traffic on the link. In case of ES20, it is also seen in case of line card reload.

  Workaround: Add and remove auto-negotiation on the interface configuration to recover the link. In case of ES20, toggling flow-control recovers the interface.

- 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.

- CSCsr72352

  Symptoms: EBGP-6PE learned IPv6 labeled routes are advertised to IBGP-6PE neighbor by setting NH as local IP address.

  Conditions: This symptom is observed on 6PE Inter-AS Option C with RR case.

  Workaround: There is no workaround.

- CSCsr76818

  Symptoms: Queue wedges on one of the SP input queues. When the peer switch was sending VTP packets to the switch trunk interface where **no vtp** was configured, the interface input-buffer was filled up by the VTP packets. When the buffer is full, the interface is not be able to process any incoming control packets.

  Conditions: Occurs when the trunk interface is configured **no vtp** and its peer interface is a has VTP enabled.

  Workaround: Configure the peer with **no vtp** to prevent VTP packets being received on the other interface.

- CSCsr79367

  Symptoms: Slow synchronization of IP subscriber sessions from Active to Standby RP.

  Conditions: This issue is observed only for a large number of IP subscriber sessions. While the traffic is flowing, if user manually requests to clear all the sessions and while that is processing the line card reboots, then standby RP can get into a state there are dangling sessions. This does not render the router useless, but increases the sync time from active to standby.

  Workaround: There is no workaround.

- CSCsr80601

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

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

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

- CSCsr81271

  Symptoms: A Cisco 7600 router with PA-A3-T3 port adapter in flexwan module WS-X6582-2PA could generate following error messages with tracebacks upon a mass ATM PVCs flap:

  ```
  SLOT 2/0: %CWAN_ATM-3-VC_OR_PORT_ERR: Invalid VCD FF03 or Port: 0 -Traceback= 403E2200
  403A8C1C 40344F88 40347FD0 403481B4 403C374C 401CD170
  ```

  Slot 2/0 is the slot the port adapter is installed.

  Conditions: This seems to only occur when a large number of ATM PVCs flap, most likely from the service provider side.

  Workaround: There is no workaround.

- CSCsr82785

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

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

  Workaround: There is no workaround.

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

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

- CSCsr82895

  Symptoms: When a router has many PPPoE sessions and the router is configured as an RP-mapping agent, the router crashes following a switchover.

  Conditions: The symptom is observed when the router has 8000 PPPoE sessions and it is configured as an RP-mapping agent. Following a switchover, the issue is seen.

  Workaround: Another router that does not have as many interfaces in the network should be configured as the RP-mapping agent.

- CSCsr84639

  Symptoms: After 30 minutes, MIB synchronization failure messages appear on primary RP. Secondary RP crashes.

  Occurs under the following scenario:

  1) Bringup 1 pppox session on the L2TP network server (LNS)

  2) Pass bidirectional traffic through the LNS

  3) After 30 minutes, MIB sync failures message appear on primary RP and secondary RP crashes.

  Workaround: Enter the **no snmp mib notification-log default** command.

- CSCsr86515

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

```
%SYS-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs
(129/17),process = Virtual Exec. -Traceback= 40B5D8A8 40B5D984 40B5DA4C 40B5DB78
40B5DC6C 40C0E1BC 4125D3A8 4209FAEC 420AA5A0 4054C05C 420570D8 40575510 41257298
41257284 %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Virtual Exec.
-Traceback= 40B5D8C8 40B5D984 40B5DA4C 40B5DB78 40B5DC6C 40C0E1BC 4125D3A8 4209FAEC
420AA5A0 4054C05C 420570D8 40575510 41257298 41257284
```

Conditions: This was observed on a Cisco 7600 with Supervisor 720 running Cisco IOS Release 12.2(33)SRB3 after a ATM sub-interface was removed.

Workaround: There is no workaround.

- CSCsr86826

  Symptoms: A standby SP may experience a memory leak in the mls-hal-agent process.

  Conditions: This has been experienced on a Cisco 7600 router with dual SUP720s running either Cisco IOS Release 12.2(33)SRC or Cisco IOS Release 12.2(33) SRC1. The router is configured for multicast.

  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.

- CSCsr97343

  Symptoms: An MSDP peer may flap randomly.

  Conditions: The symptom is observed when the device is configured with **logging host** *ip-address...* or **logging host** *ip-address*.

  Workaround: It has been observed that removing the “logging host” configuration helps in preventing the peer-flap: **no logging host** *ip-address* **no logging** *ip-address*

- CSCsr97753

  Symptoms: Pinging an interface fails.

  Conditions: Occurs when unconfiguring xconnect on the interface.

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

- CSCsr98731

  Symptoms: If running OSPF, stale routes may be installed in the RIB. Also wrong paths (inter-area vs. intra-area) are preferred.

  Conditions: Occurs on a router running Cisco IOS Release 12.2(33)SRC1.

  Workaround: There is no workaround.

- CSCsu02975

  Symptom: Router crashes due to memory corruption

  Conditions: WAN router crashes when feature combination includes Frame Relay, EIGRP, GRE, QoS, and multicast are configured on WAN aggregation and branches.

  The issue is seen only on PA-MC-2T3/E3-EC The issue is seen only when frame-relay fragment and service-policy is part of map-class frame-relay configs

  Workaround: Have either frame-relay fragment or service-policy as part of map-class frame-relay configs

- CSCsu03229

  Symptoms: On the standby provider edge (PE) aggregation device, when label allocation fails, the box can crash upon retry.

  Conditions: Occurs in redundancy mode in PE aggregation device configured for tunnel stitching.

  Workaround: There is no workaround.

- CSCsu04088

  Symptoms: With unidirectional Ethernet (UDE) enabled on ES20 port, UniDirectional Link Detection (UDLD) gets disabled. But on converting the port from L3 to L2 (or vice versa) or on shut/no shut of interface, UDLD is enabled again on the interface. Once UDLD gets enabled, due to the UDE feature, the port is detected as unidirectional and put to err-disabled state.

  Conditions: Occurs on ES20 ports configured for both UDE and UDLD.

  Workaround: Disable UDLD on the port.

- 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.

- CSCsu04473

  Symptoms: Upon the first SSO switchover triggered with the **redundancy force-switchover** command, the traffic stops on the ATM N-to-1 VCC pseudowires configured with cell-packing in the direction from the MWR towards the 7600 SPA-4XOC3-ATM interface. Traffic recovers normally in the other direction.

  Conditions: Occurs on a Cisco 7600 S-series equipped with dual SUP720-3BXL. The problem is seen only when cell-packing is enabled on the N-to-1 VCC pseudowires and when APS (MR-APS) is configured on the ATM OC3 interface of the Cisco 7600 SPA-4XOC3-ATM.

  Workaround: Disable cell-packing on the ATM N-to-1 VCC pseudowires or alternatively disable APS on the SPA-4XOC3-ATM interface.

- CSCsu05525

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

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

  Workaround: Clear the session to remove the configuration.

- CSCsu08935

  Symptoms: BGP as-override does not work properly on a PE to overwrite the AS in the AS4_PATH.

  Conditions: When a 4 byte CE is peered to a 2 byte capable PE using AS 23456 and the command **as-override** is configured on the neighbor, the PE router does not override the AS in the AS4_PATH with its own AS number, mapped to 4 bytes.

  Workaround: Use “allowas-in” on the CE.

- CSCsu09663

  Symptoms: Router crashes when scaling DHCP sessions on Cisco Intelligent Services Gateway (ISG).

Conditions: When the MCP-ISG is acting as DHCP Relay Agent or DHCP server, it crashes while large number of Layer 2-connected sessions are coming up.

Workaround: There is no workaround.

- CSCsu10229

  Symptoms: cdpCacheAddress(OID:1.3.6.1.4.1.9.9.23.1.2.1.1.4) MIB is not showing GLOBAL_UNICAST address.

  Conditions: Occurs on a Cisco 7200 router running Cisco IOS Release 12.4(15)T7.

  Workaround: There is no workaround.

- CSCsu12040

  Symptoms: BGP neighbors that are configured with as-override and send-label (CsC) together may not work after an interface flap or service reset.

  Conditions:

  ```
  neighbor xxx as-override neighbor xxx send-label
  ```
  Workaround: Enter the “clear ip bgp * soft in” command.

  Further Problem Description: Peers (neighbors) with a CsC (IPv4+label) BGP configuration with the as-override option should be separated into different dynamic update groups during the BGP update generation process. After the CSCef70161 fix in Cisco IOS Release 12.0(32)SY4, this is no longer the case; this CSCsu12040 fix enhances the CSCef70161 fix to handle the CsC (IPv4+label) case separately.

- CSCsu24087

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

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

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

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

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

- CSCsu26315

  Symptoms: Traffic may not resume on ATM over MPLS (ATMoMPLS) connections.

  Conditions: The symptom is observed when both ATMoMPLS and ATM over LS (ATMoLS) connections are on same card and a card reset is done.

  Workaround: Reload the PXF.

- CSCsu27109

  Symptoms: When stateful switchover (SSO) is performed on a Cisco 7600, MPLS label allocation fails.

  Conditions: Issues are seen on Cisco 7600 router. Occurs after performing the SSO. Also seeing CPU usage above 95% for 10-15 minutes.

  Workaround: There is no workaround.

- CSCsu27843

Symptoms: Router crashes when DHCPv6 is configured on the router.

Conditions: Router crashes when we remove the subinterface on which DHCPv6 PD request was configured.

Workaround: There is no workaround.

- 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.

- CSCsu27894

  Symptoms: Flurry of DUP_IFINDEX messages are seen on standby.

  Conditions: Occurs during bulk sync phase when standby is coming up.

  Workaround: There is no workaround.

- CSCsu31088

  Symptoms: Not able to execute any commands under interface after running BERT tests.

  Conditions: This issue is seen only after running SPA FPGA BERT tests and also when there is dual RP in chassis. With other BERT options, no issue is seen.

  Workaround: There is no workaround.

- CSCsu31935

  Symptoms: Bootup diag test failures observed on 6816 card when multirouters are reloaded. Some ports were put in error disabled state.

  Conditions: Failure triggered with random multirouters reloads (reload of CE1, PE1, Core1). Brief router info and config: IOS - 8/25 a76 Dual sup720 7606 6724 connected to remote 6724 (servicing vlans 2-2000) 6816 connected to remote 6816 (servicing vlans 2001-4000) sip600 (servicing vlans 1-4000 switchport)

  Topology:

  CE1----PE1----Core-1-----Core-2----PE2----CE2 Affected router is CE1.

  Configuration: 4k VLANs, 6816 servicing VLANs 2001-4000 (switchports).

  Workaround: Run the failing diag tests on demand.

  Further Problem Description: Few bootup tests fail when on 6816 card when the multirouters are reloaded. On failure, the ports are put in error disabled state. Failure cause has been root caused to usage of reserved diag vlans in the configs. Please refer the link mentioned below.

  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.1E/native/command/reference/S1.html

  switchport dot1q: Do not enable the reserved VLAN range (1006 to 1024) on trunks when connecting a Catalyst 6500 series switch running Cisco IOS software on both the supervisor engine and the MSFC to a Catalyst 6500 series switch running Catalyst software. These VLANs are reserved in systems running Catalyst software. If enabled, systems running Catalyst software may error disable the ports if there is a trunking channel between these systems

  When the diag vlans (1006 to 1011, 4094 to 4089) are used, there could be diag failures at some random cases. Please do not enable the reserved vlans.

- CSCsu31954

  Symptoms: A router reloads.

Conditions: Under certain crypto configurations with NetFlow also configured, the router will reload when required to fragment CEF-switched traffic on a Cisco 7200 router.

Workaround: There is no workaround.

- CSCsu32104

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

  Conditions: Unknown at this time.

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

- CSCsu35597

  Symptoms: Renaming a directory gives error message.

  Conditions: This happens on a Cisco router running Cisco IOS Release 12.4(20)T1.fc2 image

  Workaround: There is no workaround.

- CSCsu35624

  Symptoms: When a private VLAN is configured on a VTPv3 server and then deleted, the update message on a peer VTPv3 client can cause a stack overflow for VLAN manager process and crash.

  Conditions: Occurs in a Cisco 7600 running Cisco IOS Release 12.2(33)SRD.

  Workaround: There is no workaround.

- CSCsu36697

  Symptoms: The line card reloads when a line card online insertion and removal (OIR) is performed. It does not happen consistently.

  Conditions: This occurs when an empty policy is present.

  Workaround: There is no workaround.

- CSCsu36709

  Symptoms: A router may unexpectedly reload.

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

  Workaround: Do not use EIGRP to redistribute BGP.

- CSCsu36836

  Symptoms: TCL scripts and policies attempting to work with open files and sockets simultaneously may not operate properly. One symptom is the **vwait** command may fail by reporting “would wait forever”.

  Conditions: Occurs when a TCL script opens both a file and a client or server socket simultaneously.

  Workaround: Open and close files and sockets separately. Avoid having them open simultaneously.

- CSCsu37205

  Symptoms: BGP dampening under VPNv4 may cause router crash.

  Conditions: Occurs when BGP dampening is enabled on VPNv4 address family, but not on individual **IPv4 VRF**<*VRF-name*>**address-family**.

  Workaround: Enable the same set of BGP dampening on both the VPNv4 address family as well as all entries for IPv4 VRF address-family.

- CSCsu39152

  Symptoms: IF-MIB registration fails as there are no free ifIndex available.

  Conditions: Occurs after an upgrade. Seen only in HA systems.

  Workaround: There is no workaround.

- CSCsu39704

  Symptoms: Unable to configure pseudowire on virtual-PPP interface. Command is rejected with the following error:

  Incompatible with ip address command on Vp1 - command rejected

  Conditions: Occurs when IPv4 address or IP VPN routing/forwarding (VRF) has already been configured on the main interface.

  Workaround: There is no workaround.

- CSCsu40667

  Symptoms: A Cisco 7600 series router may fail to install some NetFlow entries even if NetFlow table utilization is low.

  Conditions: Occurs while flows are ingressing on ES20 module.

  Workaround: There is no workaround.

  Further Problem Description: The **show mls netflow table-contention detail** command will show a heavy ICAM table utilization, while TCAM utilization is small.

```
Router#sh mls net table-contention det
Earl in Module 1
Detailed Netflow CAM (TCAM and ICAM) Utilization
================================================
TCAM Utilization : 0%
ICAM Utilization : 98%
Netflow TCAM count : 152
Netflow ICAM count : 126
Netflow Creation Failures : 388663
Netflow CAM aliases : 0
```

- CSCsu42078

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

  Conditions: This happens when a service-policy is applied to an interface, and then service-policy is removed under certain conditions.

  One such condition is that “ip cef distributed” was configured on the router and the multi-link member flap triggered the service policy removal.

  The problem is that, after the policy was removed, the packet path vector was not reset correctly and still trying to access the already-removed policy internally. When traffic flows, it will cause crash.

  Workaround: For the above example, remove “ip cef distributed” from the configuration.

- CSCsu42315

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

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

  Workaround: There is no workaround.

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

- CSCsu44992

  Symptoms: VPDN redirect functionality does not work.

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

  Workaround: There is no workaround.

- CSCsu46822

  Symptoms: When account logon is done for a DHCP user, QoS policies defined in the user profile are not applied to the ISG session.

  Conditions: A DHCP session is created. User performs account logon via SESM (not CoA). User profile has QoS polices defined. Session is authenticated but policies are not applied to the session.

  Workaround: Perform account logon using CoA.

- CSCsu46871

  Symptoms: Unable to attach service policy to VT when bandwidth is configured in class default.

  Conditions: Occurs when DLFI over ATM is configured while trying to attach service policy to VT when bandwidth is configured in class default.

  Workaround: Configure bandwidth in user defined class and attach to VT.

- CSCsu47037

  Symptoms: Router crashes when an attempt is made to forward a packet out of an Auto-Template interface.

  Conditions: This occurs when the interface's MTU is set to 0: Use the **show interface Auto-Template X** command to show the MTU.

  Workaround: Configure a protocol MTU directly on the Auto-Template interface.

- CSCsu48898

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

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

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

- CSCsu50118

  Symptoms: More convergence time seen even with the **carrier-delay msec 0** command configured.

  Conditions: Occurs when **carrier-delay msec 0** is configured on a gigabit interface.

  Workaround: If excessive convergence time is observed even with the **carrier-delay msec 0** command configured, enter the command again on the interface.

- CSCsu51095

  Symptoms: If connected routes are optimized using PfR, there will be a routing loop.

  Conditions: This symptom can occur if, for some reason, PfR is learning connected routes or if the user has configured them.

  Workaround: Create an oer-map with a prefix-list that contains the prefixes with the IP addresses of the connected routes (the next hops). Set the set observe mode in the oer-map.

- CSCsu51245

Symptoms: Port-channel QinQ subinterface on ESM20 and SIP600 line cards do not pass traffic after router reload and line card reset.

Conditions: This condition is seen after router reload or member link line card reset. This is not seen when configuration is newly applied.

Workaround: To recover from the condition, perform a **shut/no shut** on the port channel main interface.

- CSCsu53497

  Symptoms: Traffic loss occurs in routed-PW interfaces.

  Conditions: Occurs following router bootup with highly scaled VPN, PW, and SVI configuration.

  Workaround: Perform a **shut/no shut** on SVI or on the failing interfaces.

- CSCsu54801

  Symptoms: IPv6/IPv6 Tunnel adjacency information is incomplete on the line card. This prevents IPv6/IPv6 multicast traffic on the tunnel.

  Conditions: The symptoms are observed under normal operation.

  Workaround: There is no workaround.

- CSCsu55145

  Symptoms: Router crashes due to critical software exception.

  Conditions: Occurs on a Cisco ASR 1000 running Cisco IOS Release 12.2.

  Workaround: There is no workaround.

- CSCsu55883

  Symptoms: With MLPPP configured on OSM, the following symptoms may be observed:

  1. Line card might crash.

  2. Links might flap.

  3. Following error message from line card might be seen: “SLOT 9: Sep 14 13:48:48.479 CDT: %COMMON_FIB-3-FIBIDBINCONS2: An internal software error occurred. Multilink1 linked to wrong idb R11_Mu1”

  Conditions: Occurs on routers running various Cisco IOS Release 12.2SR releases. Performing a **shut/no shut** on the OSM (especially on the card containing MLPPP) interfaces might trigger this issue.

  Workaround: There is no workaround.

- CSCsu56806

  Symptoms: Hot Standby Routing Protocol (HSRP) IPv6 configuration can be re-added to a VLAN by software after the configuration has been deleted.

  Conditions: If Hot Standby Routing Protocol (HSRP) IPv6 is configured on a VLAN interface, and the VLAN interface is deleted, then the HSRP IPv6 configuration will reappear on the VLAN if the VLAN is later recreated. Once this occurs then there is no way to remove the HSRP configuration.

  Workaround: Remove the HSRP configuration before deleting the VLAN.

- CSCsu57182

  SYMPTOM:

  The Cisco IOS may experience high CPU utilization.

  CONDITIONS:

ISAKMP is enabled.

WORKAROUND:

None.

FURTHER INFORMATION:

This issue can occur if the Cisco IOS device processes a malformed IKE message.

- CSCsu57331

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

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

  Workaround: Reset the line card.

- CSCsu57958

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

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

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

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

- CSCsu62667

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

  Conditions: Occurs following a SSO switchover.

  Workaround: There is no workaround.

- CSCsu63994

  Symptoms: With L2TPv3 sessions configured on the active RP, the CPU on standby RP is being used to setup L2TPv3 sessions to peer. The standby keeps attempting to establish all L2TPv3 sessions, which obviously fail to establish, and hence it keeps on retrying forever. This is a waste of standby RP CPU, since there is no point in attempting to establish sessions with peer on standby.

  Conditions: Occurs when L2TPv3 pseudowires are configured on a router with active and standby RPs.

  Workaround: There is no workaround.

- CSCsu63996

  Symptoms: NSF restart may be terminated and OSPF NBR may flap during RP switchover. The **debug ip ospf adj** command shows the following message: OSPF: Bad request received.

  Conditions: The symptoms are observed when the links are broadcast networks and the restarting router is DR. It is seen when “nsf cisco” is configured and when some neighbors finish OOB resync much sooner than others.

Workaround: Use the **nsf ietf** command.

Alternate workaround: Configure routers so that the restarting router is not DR (use ospf network type point-to-point or priority 0).

- CSCsu64215

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

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

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

- CSCsu64323

  Symptoms: The **show vpdn history failure** command should show the history of session failures due to entering incorrect password, but it does not show any history.

  ```
  Router#show vp hi fa % VPDN user failure table is empty
  ```
  Conditions: The problem was seen with Cisco 7201 running Cisco IOS Release 12.2(33)SRC1. No problem with Cisco IOS Release 12.4(4)XD9.

  Workaround: There is no workaround.

- CSCsu65189

  Symptoms: If router is configured as follows:

  ```
  router ospf 1 ...
  passive-interface Loopback0
  ```
  And later is enabled LDP/IGP synchronization using command

  ```
  Router(config)#router ospf 1 Router(config-router)# mpls ldp sync
  Router(config-router)#^Z
  ```
  MPLS LDP/IGP synchronization will be allowed on interface loopback too.

  ```
  Router#sh ip ospf mpls ldp in Loopback0 Process ID 1, Area 0 LDP is not configured
  through LDP autoconfig LDP-IGP Synchronization : Required < ---- NOK Holddown timer is
  not configured Interface is up
  ```
  If the **clear ip ospf proc** command is entered, LDP will keep the interface down. Down interface is not included in the router LSA, therefore IP address configured on loopback is not propagated. If some application like BGP or LDP use the loopback IP address for the communication, application will go down too.

  Conditions: Occurs when interface configured as passive. Note: all interface types configured as passive are affected, not only loopbacks.

  Workaround: Do not configure passive loopback under OSPF. Problem only occurs during reconfiguration.

  The problem will not occur if LDP/IGP sync is already in place and: - router is reloaded with image with fix for CSCsk48227 - passive-interface command is removed/added

- CSCsu65225

  Symptoms: TFTP from supervisor to ACE modules fail.

  Conditions: Results in the inability to copy/upgrade images to standby ACE. This is due to moving all 127.x.x.x addresses in an internal VPN routing/forwarding (VRF), which causes TFTP to fail.

  Workaround: ACE modules could fail-over to make standby as active and then FTP from the server directly.

- CSCsu67461

Symptoms: Router may crash when “show tracking brief” is entered if one or more tracking object have been created using the Hot Standby Routing Protocol (HSRP) cli, such as **standby 1 track Ethernet1/0**.

Conditions: This does not occur if all tracking objects use the new **track** command as follows:

track 1 interface Ethernet1/0 line-protocol interface Ethernet 0/0 standby 1 track 1

Workaround: Use **show tracking** instead, or configure tracking with the new command.

- CSCsu67637

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

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

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

- CSCsu69590

  Symptoms: After Flex Link failover, connectivity may be lost. Configured VLANs might be pruned on active link, causing VLAN interface to go down.

  Conditions: This usually happens after the second Flex Link failover.

  Workaround: Remove the Flex Link configuration from the interface, then reconfigure it.

- CSCsu71004

  Symptoms: Cisco 7600 RP crashes while executing the **copy tftp sup-bootdisk:** command. A similar crash seen upon switchover

  Conditions: Occurs when issuing a copy command from SP console on an RSP720.

  Workaround: There is no workaround.

- CSCsu71728

  Symptoms: A crash may occur while applying QOS under an MFR interface.

  Conditions: The symptoms are observed while applying QOS under an MFR interface on a PA-MC-2T3-EC in L2VPN.

  Workaround: There is no workaround.

- CSCsu72025

  Symptoms: SIP400 may crash during Change of Authorization (CoA) push.

  Conditions: Occurs on a SIP400 with ACL configurations on iEdge sessions and CoA push enabled.

  Workaround: There is no workaround.

- CSCsu73128

  Symptoms: Router crashes.

  Conditions: Occurs when large number of remote end points try to connect to the gateway at the same time. The router may crash if “rsa-sig” is used as authentication method.

  Workaround: There is no workaround.

- CSCsu74397

Symptoms: When removing PA-MC-8TE1+ from the chassis, the router has an unexpected system reload. This reload happens when you remove the port adapter and the router is running the Cisco IOS bootloader image. Also happens when the port adapter is removed after the router finishes loading the Cisco IOS bootloader image and before it loads the complete Cisco IOS Software image.

Conditions: This occurs on a Cisco 7200 VXR NPE-G2 Series Routers on the Cisco IOS bootloader image from the Cisco IOS Release 12.4(4)XD.

Workaround: Remove PA-MC-8TE1+ when the complete Cisco IOS Software Image finishes loading.

- 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.

- CSCsu77549

  Symptoms: Protocol Independent Multicast (PIM) VPN routing/forwarding (VRF) neighbors not formed.

  Conditions: Occurs after line card reload.

  Workaround: Delete and add back the MVPN configuration.

- CSCsu78559

  Symptoms: In scaled conditions (8000 IP sessions) with SACL applied, line card memory leaks over a period of 4-5 hours. Sometimes this even results in a line card crash. The “Sacl Np Client” task occupies most of the CPU, and a large number of IP sessions (around 10% of 8k) will be in feature pending status, with ACL pending flag set.

  Conditions: Occurs under scaled conditions with approximately 8000 IP sessions, with the same SACL applied to all IP sessions.

  Workaround: There is no workaround.

- CSCsu79340

  Symptoms: Cisco router crashed while Intermediate System-to-Intermediate System (IS-IS) is coming up.

  Conditions: Occurred only on a Cisco router running Cisco IOS Release 12.2(33)SRC2 with “mpls traffic-eng multicast-intact” configured under “router isis”.

  Workaround: Disable “mpls traffic-eng multicast-intact” configuration.

- CSCsu81406

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

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

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

- CSCsu81838

  Symptoms: Memory leak occurs.

  Conditions: Occurs during normal operations.

  Workaround: There is no workaround.

- CSCsu82893

  Symptoms: Features requiring nas-port as a username determined by AAA (such as pre-auth) will not work on the standby device, causing standby sessions to be poisoned.

  Conditions: AAA calculates the IP address of the best port, which is up and active. However, on the standby device, no interface is visibly active, resulting in a best IP address defining the router to be 0.0.0.0.

  Workaround: There is no workaround.

- CSCsu83563

  Symptoms: Multicast rate-limiters stop working after a HA switchover.

  Conditions: To see this issue you have to have a HA setup with multicast rate-limiters set. In order to see this issue the rate-limiters must have been set before the standby is booted. If the rate-limiters are set after standby is up in HOT state, the issue is not seen after switchover.

  Workaround: Remove and reconfigure the rate-limiters.

- CSCsu83588

  Symptoms: After a router reload, the Flex Link configuration (**switchport backup interface Po#**) is lost.

  Conditions: Occurs when a backup interface is a port-channel interface.

  Workaround: There is no workaround.

- CSCsu87248

  Symptoms: Router crashes while adding flexible NetFlow.

  Conditions: Occurred on a router running Cisco IOS Release 12.2(33)SRC1.

  Workaround: There is no workaround.

- CSCsu88256

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

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

  Workaround: There is no workaround.

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

- CSCsu89550

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

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

  Workaround: Remove the control-plane policy.

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

- CSCsu90280

  Symptoms: IPv6 DMVPN tunnel does not work. IPv6 NHRP registration between Hub and Spoke fails.

  Conditions: The symptoms are observed under normal operation.

  Workaround: There is no workaround.

- CSCsu92966

  Symptoms: Send statistics from the **show mpls l2 vc** command are not displayed.

  Conditions: Occurs on a PE when the other PE's core-facing link is flapped.

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

- CSCsu93374

  Symptoms: The group state of a slave group may unexpectedly change to Active after an RP switchover.

  Conditions: The symptom is observed when HSRP multigroup is configured such that a slave group follows the state of a master group. If the HSRP group state is Standby, then the group state of the slave group may change to Active after an RP switchover.

  Workaround: There is no workaround.

- CSCsu94030

  Symptoms: Internal VRF gets disabled at when the router boots up.

  Conditions: Occurs after any failover or router start-up scenario

  Workaround: Use the **no platform ivrf disable** to avoid the issue.

- CSCsu94720

  Symptoms: Router crashes when the **shutdown** command is used on an interface.

  Conditions: Occurs when there are DHCPv6 bindings.

  Workaround: There is no workaround.

- CSCsu94864

  Symptoms: The MLS shortcut for a user-traffic flow based on RADIUS Framed-IP (FIP) is not purged when the FIP sticky times out. RADIUS Load Balancing (RLB) sends out a purge request before deleting sticky and has no effect in deleting the MLS shortcut entry.

  Conditions: Occurs on a device configured with RLB and FIP sticky idle timer and with MLS aging timer configured higher than the RLB FIP sticky idle timer.

  Workaround: There is no workaround.

- CSCsu95080

  Symptoms: A router remains in the init_process state when parsing the configuration.

  Conditions: The symptom is observed when an IPv6 multicast group joins without MLD configured. When the groups unjoin, the system suspends.

  Workaround: Configure MLD.

- CSCsu95171

  Symptoms: In switches running Cisco IOS Release 12.2(33)SRC, high CPU may be seen on the SP/DFC due to NDE-IPv4 process. This may result in following unrelated problems:

  - Corrupted file system(s)

  - **show running** command may show "read error" etc.

  - Continuous CPUHOGs automatically disabling Cisco Express Forwarding (CEF).

  Log Messages reported:

  ```
  %SYS-SP-3-CPUHOG: Task is running for (4000) msecs, more than (2000)msecs
  (2/0),process = NDE - IPV4.
  ```

  Conditions:

- Affects 12.2(33)SRC or later, but not earlier versions.

- Slow response to console commands.

- Netflow enabled on point-to-point interfaces

- High number of IPv4 routes learned via BGP.

Workaround: Downgrade to the latest release of 12.2(33)SRB. During high CPU condition, do the following:

1. Remove ALL interface level and global netflow configurations.

2. Configure global command: **cef table output-chain build favor convergence-speed**.

3. Re-apply global and interface level netflow configurations.

The **cef table ...** command mentioned above will stay in the configuration. This command should stop this issue from re-occurring.

- CSCsu95319

  Symptoms: Igmp-proxy reports for some of the groups are not forwarded to the helper. This causes members not to receive the multicast traffic for those groups.

  Conditions: The problem is seen when the igmp-proxy router is receiving UDP control traffic. That is, the router is receiving any UDP control-plane traffic on any interface.

  Workaround: There is no workaround.

- CSCsu96649

  Symptoms: On Cisco 7600 with RSP720-3C-10GE processor, if the SIP-400 is configured as Lawful Intercept (LI) service module after a line card online insertion and removal (OIR), the SIP-400 may not get selected as Lawful Intercept service module.

  Conditions: Occurs when the SIP-400 is configured as Lawful Intercept service module on the Cisco 7600.

  Workaround: After line card OIR, select the SIP-400 again as the LI service module using the command **li-slot list** <*sip400 slot number*>.

- CSCsu96730

  Symptoms: Intelligent Services Gateway (ISG) traffic from one user to another may fail if the packet needs to be processed by the RP in a Cisco 7600.

  Conditions: Occurs when ISG is configured and packets are switched from one subscriber to a second subscriber.

  Other symptoms : - Counters of packet transfer might show difference between user transferring between each other - Access-list might fail to block the packet

  The 2 above symptoms will be seen when user are sending receiving on the same interface via the ISG

  Workaround: There is no workaround.

- CSCsu97934

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

  Conditions: Unknown.

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

- CSCsu99573

Symptoms: Cisco router crashes when Open Shortest Path First (OSPF) neighbor is being configured in non-base topology and IP address of the neighbor does not fall into range of any existing interface.

Conditions: This crash will only occur when OSPF is configured to support multi-topology routing, and neighbor statements are used in the submode for a non-base topology.

Workaround: Configure the neighbor with this IP address in the base topology first.

- CSCsv00168

  Symptoms: Junk values are being displayed on the router when characters/commands are inputted. For example, enter “enable”, it shows “na^@^@”; enter “show version”, it shows “h ^v^@e^@^r^@^@^@^@^@”.

  Conditions: The symptoms are observed with Cisco IOS Release 12.4(23.2)T.

  Workaround: There is no workaround.

  Further Problem Description: The CLI function is not affected by the junk values.

- CSCsv01474

  Symptoms: The **ip rip advertise** command might be lost from the interface.

  Conditions: This symptom occurs in any of the following three cases:

  1. The interface flaps. 2. The **clear ip route** command is issued. 3. The **no network <prefix>** command and then the **network <prefix>** command are issued for the network corresponding to the interface.

  Workaround: Configure the **timers basic** command under the address-family under rip.

- 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.

- CSCsv03300

  Symptoms: Cisco 7200 NPEG2 router crashes while displaying the interface output for onboard gigabit ethernet using the **show interface gig0/x** command.

  Conditions: Occurs when a CBWFQ QoS policy is attached to the onboard gigabitethernet interface.

  Workaround: There is no workaround.

- CSCsv04674

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

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

  Workaround: There is no workaround.

- CSCsv04733

  Symptoms: A LAC might terminate a tunnel unexpectedly.

  Conditions: This symptom is seen when the tunnel password exceeds 31 characters.

  Workaround: Use a shorter password if policy allows.

Further Problem Description: This is seen with Cisco IOS interim Release 12.2 (34.1.3)SB1. With a customer specific special based on Cisco IOS Release 12.2 (31)SB11, it allowed 64 characters.

- CSCsv05934

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

  Workarounds:There are no workarounds available for this vulnerability.

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

- CSCsv06309

  Symptoms: Link debounce down feature not working on RSP720-3C-10GE ports due to fast link feature.

  Conditions: Occurs when link debounce is configured on RSP720-3C-10GE.

  Workaround: Use "carrier-delay" instead.

  Further Problem Description: On configuring link debounce, fast link, which is enabled by default and has no CLI, needs to go off but does not.

- CSCsv06608

  Symptoms: SXP is set up between two devices but fails to initialize.

  Conditions: This symptom is observed when SXP is set up between two devices.

  Workaround: There is no workaround.

- CSCsv07188

  Symptoms: Unable to configure PVC when **connect** command is configured.

  Conditions: Occurs Cisco 7200 routers.

  Workaround: There is no workaround.

- 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.

- CSCsv08528

  Symptoms: After the Resilient Ethernet Protocol (REP) topology is returned by the **rep preempt** command, MAC address table is not cleared.

  Conditions: During internal testing, this occurred approximately 3 times out of 20.

  Workaround: Use the **clear mac-address-table dynamic** command to clear the table.

- CSCsv13243

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

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

  Workaround: Configure subinterface in "non-native" mode.

- CSCsv13738

  Symptoms: There are two ways to define VRFs when supporting the 6VPE feature: 1) ip vrf 2) vrf definition. The “vrf definition” configuration may take a much longer time to allow convergence between the PE and the CE than the “ip vrf” configuration.

  Conditions: The symptoms are observed under the following conditions: - when the router boots up; and - when the issue has been seen using the “vrf definition” configuration; and - when the router has over 100,000 VPNv4 BGP routes; and - when a large number of VRFs are configured.

  Workaround: Use the “ip vrf” configuration, if you have only IPv4 VRFs configured.

- CSCsv13914

  Symptoms: Traceback observed when the PPPoEoA session is brought up.

  Condition: Occurs when the interface is not up.

  Workaround: There is no workaround.

- CSCsv14963

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

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

  Workaround: There is no workaround.

- CSCsv15040

  Symptoms: Infinite Loop occurs when doing MIB walk on cdot1agStackTable objects.

  Conditions: Occurs on a Cisco 7600 running Cisco IOS Release 12.2(33)SRD and configured with 10GE-XFP-SPA and SIP-600 configured for Distributed Forward. This problem is seen when “MIP/MEP” configured on Te1/0/0 interface and MIB walk is performed on cdotagStackTable objects.

  Workaround: Do not configure “MIP/MEP” on Te1/0/0 interface.

- CSCsv16869

  Symptoms: BGP updates may not be sent out.

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

  Workaround: There is no workaround.

- CSCsv20125

  Symptoms: PPPoE sessions over VLAN over ATM with process switch stuck at LCP stage.

  Conditions: Occurs when the **protocol pppovlan** command is configured on ATM subinterface along with **no ip cef**. PPPoE sessions are not created.

  Workaround: Use the **ip cef** command.

- CSCsv21295

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

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

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

- CSCsv21403

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

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

  Workaround: There is no workaround.

- CSCsv22930

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

  Conditions: Occurs when pseudowire stitching is configured.

  Workaround: Do not enable FRR between these routers.

- CSCsv23252

  Symptoms: A Cisco 7600 running Virtual Private LAN Services (VPLS) with QinQ tunnels is forwarding CDP/VTP packets from the tunnel interfaces across remote sites, even when L2TP is not enabled.

  Conditions: Occurs with a VPLS setup with QinQ tunnel interfaces facing the customer edge.

  Workaround: Use different domain names to avoid changes to VTP database.

- CSCsv24179

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

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

  Workaround: There is no workaround.

- CSCsv24908

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

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

  Workaround: Reload the chassis.

- CSCsv25306

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

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

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

- CSCsv27428

  Symptoms: TCP sessions passing through a NAT router freeze.

  Conditions: The NAT router is a Cisco 7600 with RSP720. NAT translation entries keep using syn-timeout (default = 60 sec) even after TCP three-way handshake is done. Use **show ip nat translation verbose** to check timer

  Workaround: Use the **ip nat translation syn-timeout** command, which mitigates the problem to some extent.

- CSCsv27617

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

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

  Workaround: Remove and reconfigure NetFlow on the affected interfaces.

- CSCsv28451

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

  ```
  E2#sh ip route vrf foo 10.5.5.5
  Routing Table: foo Routing entry for 10.5.5.5/32 Known via "ospf 1", distance 110,
  metric 20, type extern 2, forward metric 10 Redistributing via bgp 666 Advertised by
  bgp 666 metric 10 match internal external 1 & 2 Last update from 10.45.45.2 on
  Ethernet1/0, 00:00:56 ago Routing Descriptor Blocks: * 10.45.45.2, from 10.5.5.5,
  00:00:56 ago, via Ethernet1/0 Route metric is 20, traffic share count is 1 PE2# PE2#sh
  ip bgp vpnv4 vrf foo 10.5.5.5 % Network not in table PE2#
  ```

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

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

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

- CSCsv29659

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

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

  Workaround: There is no workaround.

- CSCsv30307

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

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

  Workaround: There is no workaround.

- CSCsv30540

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

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

  Workaround: There is no workaround.

- CSCsv33977

  Symptoms: BGP peer fails to exchange the OPEN Message for negotiating capability when the neighbor router does not support any BGP capabilities.

  Conditions: The symptom is observed when the neighbor router does not support any BGP capabilities and when the capability negotiation fails due to an SSO switchover.

  Workaround: Configure “neighbor x.x.x.x dont-capability-negotiate". Issue the **clear ip bgp *** command when the issue occurs.

- CSCsv35120

  Symptoms: The ES20-GE3C/GE3CXL line card may crash if the explicit-path of an MPLS Traffic Engineering (TE) tunnel is changed so that it no longer goes out a core-facing port-channel interface.

  Conditions: Seen only when the following conditions are met:

  - Virtual Private LAN Services (VPLS) traffic passes over the MPLS Traffic Engineering tunnel.

  - Traffic going out the tunnel initially goes over a port-channel interface.

  - Five or more ports on the ES20 line card are used in the port-channel interface.

  - The explicit-path specified avoids the port-channel interface

  Workaround: Shut down the port-channel interface first before changing the tunnel's explicit-path.

- CSCsv36266

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

  Serial1/0/0.1/2/1/1:1 ifOperStatus.156 = up(1)

  E1 1/0/0.1/2/1/1 ifOperStatus.157 = lowerLayerDown(7

  TU 1/0/0.1/2/1/1 ifOperStatus.158 = down(2)

  tug 3-2 tug 2-1 e1-1:chgrp1

  AU-4 1, TUG-3 2, TUG-2 1, E1 1 (C-12 1/2/1/1) is up

  156 Se1/0/0.1/2/1/1:11500512KUP UP

  157 E1 1/0/0.1/2/1/102.05MUP <blank>

  158 TU 1/0/0.1/2/1/102.05MUP down

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

  Workaround: There is no workaround.

- CSCsv36892

  Symptoms: TCLsh mode is not exited when the session is disconnected or times out. The next user to connect and authenticate is put in TCLsh mode.

  Conditions: Occurs on high availability systems with an active and standby RP.

  Workaround: Explicitly exit TCLsh mode rather than disconnecting or allowing the session to time out.

- CSCsv38166

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

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

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

Cisco has released free software updates that address this vulnerability.

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

This advisory is posted at the following link:

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

- CSCsv41886

  Symptoms: Entering the **no ip routing** or **no router bgp xx** command yields the following error message:

  ```
  %IPRT-3-IPDB_DEL_ERROR: i_pdb delete error bgp, 4, 210074C8, 20E322E0, 0, 0 -Process=
  "IP RIB Update", ipl= 0, pid= 117, -Traceback= 0x61FD7F58 0x62005498 0x62006D24
  ```

  Conditions: Occurs when a large number of VRFs must be configured and BGP is also configured to support these VRFs, then a **show** command, such as **show run**, is issued shortly after the **no ip routing** or **no router bgp** command.

  Workaround: There is no workaround.

- CSCsv42176

  Symptoms: Router reloads, and the following error is displayed:

  ```
  SP: MACSEC: Assert failure: mat_rc >= BD_MAT_RET_SUCCESS
  ```

  Conditions: Occurs when, for a given service instance, a secure entry is removed with **mac security aging** *inactivity* configured and **mac security** configured.

  This can occur through the CLI via a command like **clear ethernet service instance id** *id interface interface id* mac table, or it can occur due to EFP shutdown.

  If this occurs at the same time that the entry's aging timer expires, the reload may occur.

  Workaround: There is no workaround if "aging inactivity" is required. This problem will not occur if **mac security aging** *inactivity* is not configured.

- CSCsv48296

  Symptoms: The router reloads with the following error:

  SYS-6-BLKINFO: Corrupted redzone blk

  Conditions: Occurs when the **cns image** is active, and a CNS image operation is in progress.

  Workaround: There is no workaround.

- CSCsv50159

  Symptoms: Spurious access or crash seen on a router with a CEoP SPA, when bulk sync happens between RP and RPR.

  Conditions: Occurs during regular bootup.

  Workaround: There is no workaround.

- CSCsv50606

  Symptoms: Subsequent software releases are not backward compatible with Cisco IOS Release 12.2(33)SXI when performing an ISSU upgrade.

  Conditions: Occurs with versions of Cisco IOS that are released after Cisco IOS Release 12.2(33)SXI.

  Workaround: Instead of ISSU upgrade or downgrade, perform a regular image upgrade or downgrade.

- CSCsv57587

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

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

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

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

- CSCsv59031

  Symptoms: SIP-400 crashes on RADIUS CoA push with Cisco Intelligent Services Gateway (ISG).

  Conditions: Occurs on a SIP-400 configured for IP/PPPoE sessions and ACL configuration push from other router.

  Workaround: There is no workaround.

- CSCsv62150

  Symptoms: When cbgpPeerCapsTable is queried, it does not return the results of VPNv4 neighbors.

  Conditions: Configuration should have VPNv4 neighbors.

  Workaround: There is no workaround.

- CSCsv63799

  Symptoms: A router may reload if PfR is enabled and the number of flows exceeds the size of the NetFlow cache. This is a stress condition.

  Conditions: This symptom is observed when PfR is enabled (which also enables NetFlow).

  Workaround: A possible workaround is to configure the following:

  ip flow-cache timeout active 1

- CSCsv66827

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

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

  Workaround: There is no workaround.

- CSCsv73388

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

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

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

- CSCsv73509

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

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

Workaround: There is no workaround.

- CSCsv73735

  Symptoms: After performing a redundancy switchover (RPR+ mode), the ARP table is not correctly populated. Entering the **clear ip arp** or the **clear arp-cache** commands, then pinging the connected CE or PE causes an incomplete entry to be added to the ARP table.

  Conditions: This is seen on Gigabit Ethernet, FastEthernet and POS interfaces. ATM and serial interfaces seem do not appear to be affected. This behavior is not seen with stateful switchover (SSO).

  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.

- CSCsv79584

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

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

  Workaround: There is no workaround.

  Further Problem Description: This behavior can indirectly have a negative impact on the system by triggering other applications to be called because the routing table change is triggered by such DHCP requests. Examining “debug ip routing” for 0.0.0.0/32 reveals 0.0.0.0/32 route flapping.

- CSCsv79673

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

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

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

- CSCsv79993

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

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

  router eigrp 10

  network 10.0.0.0

  distribute-list 49 out Ethernet1/2.10

router rip

network 10.0.0.0

default-metric 2

distribute-list 49 out Ethernet1/2.10

Workaround: There is no workaround.

- CSCsv80014

  Symptoms: When doing an SNMP walk on OLD-CISCO-IP-MIB when the routing table has several thousand prefixes, excessive CPU utilization occurs.

  Conditions: The symptoms are seen only when there are several thousand prefixes in the routing table.

  Workaround: Exclude the OLD-CISCO-IP-MIB from the SNMP walk. This MIB has been deprecated.

- CSCsv81009

  Symptoms: Intermittent traffic loss occurs on switch virtual interface (SVI) enabled with Virtual Router Redundancy Protocol (VRRP). Cannot ping VRRP IP address.

  Conditions: Occurs with VRRP configured on SVI. Traffic loss/ping VRRP IP address failure seen sometimes on bootup.

  Workaround: If VRRP mac-address is present as dynamic entry on bootup, this issue can be seen. Reconfigure VRRP as a workaround.

- CSCsv81751

  Symptoms: Cisco 7200 G2 router crashes when changing configuration of serial interfaces from PPP to SDLC and back to PPP, while running traffic.

  Conditions: This is observed on a T3 link with 56 channel groups configured on a WAN aggregation device. All the serial interfaces have service-policy configured.

  Workaround: Remove the service-policy before changing the encapsulation to SDLC.

- CSCsv85530

  Symptoms: When accounting is enabled for virtual private dial-up network (VPDN), there might be messages with termination cause “nas-error” and displaying impossible values in Acct-Input-Octets, Acct-Output-Octets, Acct-Input-Packets and Acct-Output-Packets.

  This causes accounting to be unreliable.

  Conditions: Occurs with Cisco IOS Release 12.4T and configured for PPTP/L2TP with accounting.

  Workaround: There is no workaround.

- CSCsv85990

  Symptoms: If there are multiple EFPs with, for example encapsulation 100, same encapsulation on different interfaces and with different bridge-domains configured for Virtual Private LAN Services (VPLS), then if there is a topology change notification (TCN) received on one of the Ethernet Flow Points (EFPs) on one interface, then Label Distribution Protocol (LDP) MAC address withdrawals are sent for all the bridge domains on all the interfaces.

  Conditions: Occurs when the network has EVCs on the L2-Access forwarding to VPLS core. Multiple Spanning Tree (MST) is running on the access VLANs.

  Workaround: There is no workaround.

- CSCsv86256

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

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

Workaround: Disable FRR at the stitching point.

- CSCsv86288

  Symptoms: Sending a NETCONF hello reply which contains a “session-id” element triggers an instant crash. The device will report a reload due to a bus error.

  Conditions: This occurs when sending a hello reply which contains a session-id element. A hello without this element, one which only contains NETCONF capabilities, does not cause a crash.

  Workaround: Send a NETCONF hello without a session-id element.

- CSCsv89643

  Symptoms: If Ethernet interface configured as Open Shortest Path First (OSPF) point-to-point network then adjacency is being established using only multicast packets. As a result routes calculated over the link do not have MAC address of next-hop’s IP resolved prior to routes being installed into the routing table. This leads to delay for routes to become usable as lower-level protocols have to trigger MAC resolution. During short period of time traffic sent over the interface is lost when routes are just installed for the first time.

  Conditions: Occurs when Ethernet interface is configured for OSPF point-to-point.

  Workaround: Problem will self-correct because passing traffic triggers MAC address resolution.

- CSCsv90323

  Symptoms: ISSU upgrade to Cisco IOS Release 12.2(33)SRD did not put router into route processor redundancy (RPR) mode.

  Conditions: Occurs when **no service image-version efsu** is enabled. During ISSU upgrade from Cisco IOS Release 12.2(33)SRB or SRC to Cisco IOS Release 12.2(33)SRD, the router incorrectly goes into stateful switchover (SSO). The correct mode is RPR because SSO ISSU from these releases to Cisco IOS Release 12.2(33)SRD is not supported.

  Workaround: Remove the **no service image-version efsu** configuration by the default **service image-version efsu** and continue the upgrade process.

  Further Problem Description: If any of the following Config, Exec or ROMMON variables are set, the SSO-based ISSU will not be blocked:

  Config:

  “no service image-version efsu”,

  “no service image-version compatibility”,

  Exec:

  “issu image-version compatibility disable”,

  ROMMON variable:

  RED_MODE = “RPR_PLUS’

  RED_MODE_SSO

  RF_REDUN_COMP = 1

  When performing any ISSU upgrade from SRB/SRC to SRD, make sure none of the above overrides is set on the router. The **service image-version efsu** command detects the incompatibility and puts the router in RPR mode.

- 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.

- CSCsv92088

  Symptoms: BACKPLANE_BUS_ASIC-4-DEV_RESET error interrupts generated by SIP-400 module, causing traffic interruption.

  Conditions: Occurs when PPPoE traffic ingresses a SIP-400 line card on a Cisco 7600 Series router running Cisco IOS Release 12.2SR.

  Workaround: There is no workaround.

- CSCsv94471

  Conditions: On an ES-20, sometimes the interface configured as a promiscuous port does not forward the traffic to other community and isolated ports on the same private VLAN. The traffic on the promiscuous port is forwarded to all other community and isolated ports belonging to the same private VLAN. This is the expected behavior.

  Condition: Sometimes using the CLI on the interface configured in the promiscuous mode **switchport mode private-vlan promiscuous** after **switchport private-vlan mapping <primary vlan> <secondary vlans>** can cause traffic to be dropped. The order of these CLIs should not matter.

  Workaround: There is no workaround.

- CSCsv97273

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

  Signal = 11 Vector = 0x1400

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

  Workaround: There is no workaround.

- CSCsv99716

  Symptoms: A Cisco 10000 series router may crash at issu_print_memory while doing a loadversion.

  Conditions: The symptom is observed on a Cisco platform, when enabling the debug command **debug issu all** in the router and doing a loadversion.

  Workaround: Do not turn on ISSU debug.

- CSCsw14845

  Symptoms: An access-list with multiple ports in a single entry only programs the first port into TCAM. All subsequent ports are not processed according to the access-list entry.

  For example, the following access-list should block both SSH (TCP port 22) and Telnet (TCP port 23), but Telnet is permitted.

  ```
  ip access-list extended deny_ssh_and_telnet deny tcp any any eq 22 telnet permit ip
  any any
  ```

  Conditions: Occurs when there is an extended named access-list with multiple ports in a single access-list entry. This only applies to transit traffic since traffic destined to the router is process-switched and processed in software.

  Workaround: There is no workaround.

- CSCsw16698

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

  Other Symptoms:

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

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

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

  1.3 Output of "show run" is delayed.

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

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

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

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

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

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

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

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

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

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

- 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.

- CSCsw24611

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

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

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

Workaround: There is no workaround.

- CSCsw24826

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

  Conditions: Crash is specific to the following scenario:

  1. Neighbor router performs IETF NSF restart.

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

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

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

  1) Shutdown OSPF interface

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

  - NO => good, remove interface

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

  3) Repeat Step 1.

- CSCsw25255

  Symptoms: A Catalyst 6500 or Cisco 7600 router may not send back a BPDU with agreement flag in response to a proposal on its root port, causing slow convergence on the designated bridge.

  Conditions: This is seen on Catalyst 6500 switches running any version of Cisco IOS Release 12.2(33)SXH. This is seen on Cisco 7600 routers running any version of Cisco IOS Release 12.2SR.

  Workaround: The problem does not occur if **debug spanning-tree event** is enabled. This can be a suitable workaround in an environment with a small number of VLANs if the debug does not impact CPU usage.

- CSCsw28082

  Symptoms: SNMP messages are not seen.

  Conditions: When the BRI interface is down on a remote router, and **no ppp link reset** is configured on device, SNMP trap message shows "down" instead of "keepalive failed".

  Workaround: There is no workaround.

- CSCsw28139

  Symptoms: PBR stops working after stateful switchover (SSO). All traffic that should be policy routed is dropped instead.

  Conditions: This usually happens after several switchovers between supervisors. Usually problem occur after about 10 switchovers, however, it could happen after first one.

  Workaround: Remove and add policy on the interface.

- CSCsw31019

  Symptoms: A Cisco router crashes.

Conditions: This symptom is observed if the **frame-relay be 1** command is issued under "map-class frame-relay <name>" configuration.

Workaround: There is no workaround.

- CSCsw35155

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

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

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

- CSCsw35638

  Symptoms: When a Cisco router is the Merge Point (MP) for a protected TE tunnel, and FRR is triggered, two things happen:

  - The primary LSP goes down, and traffic is lost on the protected tunnel. - Any PLR that is downstream of the failure will lose its backup.

  Conditions: When a competitor's router is a point of local repair (PLR) and a Cisco router is a merge point, then when FRR is triggered, the Cisco router drops the backup tunnel (in some cases immediately and in other cases after 3 minutes). This causes the primary tunnel that is protected by this backup to go down. The issue has been identified as related to the fact that session attribute flags (link/node protection desired) are being cleared by the competitor PLR when the Path is sent over the backup tunnel.

  Workaround: There is no workaround.

- CSCsw36285

  Symptoms: The **show policy-map interface** command yields incorrect policer information.

  Conditions: This problem affects only the reporting of policing statistics. It does not affect policer functionality. When police action is configured in a service-policy, the conformed rate displayed in **show policy-map interface** does not match with the class-map offered rate.

  Workaround: There is no workaround.

- CSCsw36872

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

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

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

- CSCsw37053

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

  Conditions: Occurs under the following scenario:

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

2. The recirculation VLAN has the wrong VPN number.

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

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

- CSCsw37635

  Symptoms: A Cisco 10000 series router may crash at issu_print_memory while doing a loadversion.

  Conditions: The active router crashes when doing load version with “debug issu all” turned on.

  Workaround: Do not turn on ISSU debug.

- CSCsw43211

  Symptoms: Following errors are seen:

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

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

  Workaround: There is no workaround.

- CSCsw43272

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

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

  Workaround: Use IP pool instead of DHCP pool.

- CSCsw43499

  Symptoms: Accounting start sent on DHCP OFFER rather than ACK.

  Conditions: This issue can cause accounting irregularities if the DHCP process does not complete. For example, with active-active Cisco Intelligent Services Gateway (ISG) redundancy, two DHCP OFFERs will be sent, but only one will be accepted. Since accounting records are generated for both OFFERs, they will be duplicates of each other.

  Workaround: There is no workaround.

- CSCsw43948

  Symptoms: A Cisco 3845 router that is running Cisco IOS Release 12.4(13) may bounce the frames (which are not destined for itself) on the same interface that receives them.

  Conditions: The symptom is observed if there is bridging configured on an ethernet subinterface in the following way:

  ```
  ip cef ! bridge irb ! interface GigabitEthernet0/1 no ip address no sh ! ! interface
  GigabitEthernet0/1.100 encapsulation dot1Q 100 ip address x.x.x.x x.x.x.x no ip
  redirects no ip unreachables no ip proxy-arp ip rip advertise 10 ! interface
  GigabitEthernet0/1.509 encapsulation dot1Q 101 bridge-group 1
  ```

  Workaround: If the command **bridge-group 1** is removed from the sub-interface, it will behave as expected.

- CSCsw47475

  Symptoms: Cisco 7600 router has multiple E1s that randomly flap.

  Conditions: Occurs on a router with RSP720, SIP-200 and 8xCHT1/E1 SPA installed.

Workaround: There is no workaround.

- CSCsw50608

  Symptoms: With the traffic flowing between a promiscuous port and a port belonging to a community VLAN of the same primary VLAN, if the user adds or removes any other secondary VLAN under the same private VLAN using the following configuration under “int gi” for the promiscuous port.

  Conditions: The issue was seen upon using the following CLI on the interface configured in the promiscuous mode.

  switchport private-vlan mapping*primary-vlan* **add/remove***secondary-vlan*.

  Workaround: There is no workaround.

- CSCsw52698

  Symptoms: The following error message is displayed:

  %BACKPLANE_BUS_ASIC-4-DEV_RESET: Backplane Bus Asic reset, interrupt [0x062D]=0x0008

  Conditions: Symptom reported by 7600-SIP-400 cards on 7600 Series Routers when PPPoE connections are terminated via the 7600-SIP-400 cards.

  Workaround: There is no workaround.

- CSCsw53404

  Symptoms: FR-FR and FR-Ethernet connections configured for anything over MPLS (AToM) interworking do not work with the combination of SIP400 and channelized SPAs.

  Conditions: Occurs with Frame Relay AToM configurations with SIP400 and channelized SPAs.

  Workaround: There is no workaround.

- CSCsw62346

  Symptoms: When unsupported filter is added to global policy-map with only match-any as the filter, the router or line card might crash.

  Conditions: Occurs when global policy map is attached to an interface.

  Workaround: Detach service policy from interface before making changes.

- CSCsw63003

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

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

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

- CSCsw64270

  Symptoms: Traffic may stop flowing on a T1 interface configured with Frame-relay encapsulation on online insertion and removal (OIR) of the SIP-400.

  Conditions: The problem was observed on a Cisco 7600 router with Sup720 and SPA-1XCHOC12/DS0 installed in a SIP-400. The traffic may not recover on a T1 interface configured for Frame-relay encapsulation after an OIR of the SIP-400.

  Workaround: Perform a software reset of the SIP-400 or reload of the router.

- CSCsw69366

Symptoms: When sending packets that exceed specified MTU, packets are received as giants in PA-T1/E1 IMA card instead of being fragmented.

Conditions: It happens only after changing sub-interface MTU and after stateful switchover (SSO).

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

- CSCsw70125

  Symptoms: A Cisco 7600 SIP-400 with POS interfaces encapsulated with IETF frame-relay may incorrectly set 0x800 as Network Layer Protocol Identifier (NLPID) for hardware assisted multicast IP packets. The correct value is 0xCC.

  Conditions:

  A. IP unicast packets in hardware path do not have this problem.

  B. IP multicast or unicast packets in software path do not have this problem.

  C. Problem reproducible in Cisco IOS Release 12.2(33)SRA2, 12.2(33)SRA7, and 12.2(33)SRC2.

  Workaround: There is no workaround.

- CSCsw71208

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

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

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

- CSCsw72677

  Symptoms: Router crashes with “no bba-group pppoe”.

  Condition: Happens after unconfiguring “bba-group”.

  Workaround: There is no workaround.

- CSCsw73863

  Symptoms: IDs allocated from DHCP are leaked, causing the device to reload.

  Conditions: Device is configured as Cisco Intelligent Services Gateway (ISG) DHCP with 24000 sessions flapping every 10-12 minutes.

  Workaround: There is no workaround.

- CSCsw73956

  Symptoms: During health monitor failure, platform action was taken immediately but platform action should be taken from gold TCL policy.

  Conditions: Occurs when health monitor test failure crosses failure threshold.

  Workaround: There is no workaround.

- CSCsw75589

  Symptoms: If you have configured Netflow and also have “ip flow-cache mpls label-positions”, you are very likely to run in a bus error crash with info similar to what is seen here:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address 10:28:28 UTC Sat Dec 20 2008
  addr=0x1E, pc=0x61CB7180, ra=0x61CBA5C0, sp=0x65BCAF20
  %ALIGN-1-FATAL: Illegal access to a low address 10:28:28 UTC Sat Dec 20 2008
  addr=0x1E, pc=0x61CB7180, ra=0x61CBA5C0, sp=0x65BCAF20
  10:28:28 UTC Sat Dec 20 2008: TLB (store) exception, CPU signal 10, PC = 0x61CB7180
  ```

  Conditions: Problem is platform independent but specific to IOS release. This problem is seen in 12.2(33)SRC1 and possibly affects 12.4T releases as well.

Workaround: Consider removing MPLS netflow configuration by removing the **ip flow-cache mpls label-postion 1** command.

- CSCsw76113

  Symptoms: Unable to reuse a sub-interface as main-interface.

  Conditions: Occurs when we configure **no virtual-template subinterface** when all of the Interface Descriptor Blocks (IDB) that platform supports are used as “subif-vaccess”. No more “vaccess” can be created.

  Workaround: Do not configure **no virtual-template subinterface** at run time. Check **show vtemplate** output. If there are more IDBs used by subinterface, then do not configure **no virtual-template subinterface**.

- CSCsw76910

  Symptoms: Supervisor reloads on configuring or verifying firewall farm commands.

  Conditions: Occurs before and after compliance testing on the firewall farm commands.

  Workaround: There is no workaround.

- CSCsw77205

  Symptoms: ES20 line cards crashing in a loop while using a anything over MPLS (AToM) VC with Cisco Intelligent Services Gateway (ISG).

  Conditions: The issue is seen on all the ES20 cards installed in a Cisco 7609 router running Cisco IOS Release 12.2(33)SRC2.

  Workaround: Manually shutdown the AToM interfaces and ISG interfaces to stop the crashes.

- CSCsw78413

  Symptoms: The BFD configuration may be lost from the interface/sub-interface upon a router reload or physical module of OIR.

  Conditions: The symptom is seen when BFD is configured on an interface in certain multi-slot chassis.

  Workaround: Ethernet interfaces seem immune to this problem. Certain platforms, such as the Cisco 10000 series router, are also immune.

- CSCsw78939

  Symptoms: No new sessions can come up using VPDN after a few days.

  Conditions: The root cause is that we leak and run out of SSM switch IDs.

  Workaround: There is no workaround.

- CSCsw81485

  Symptoms: Issuing **no** form of IPX configuration commands on an interface crashes the switch.

  Conditions: Occurs when IPX routing is enabled on the device but not on the interface.

  Workaround: Do not issue **no** form of IPX configuration commands on an interface where IPX is not enabled.

- CSCsw82462

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

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

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

- CSCsw82507

  Symptoms: DPM on secondary Cisco Intelligent Services Gateway (ISG) does not clear its session despite the fact that a DHCP termination message is sent. Even though the binding is cleared, the session persists until the idle timeout expires or the session is manually cleared.

  Conditions: Occurs when multiple DHCP relay agents are present between clients and DHCP server.

  Workaround: The session may expire due to idle timeout or be manually cleared.

- CSCsw85986

  Symptoms: Traffic through multilinks drop in one direction as some bundles show lost fragments, causing input errors to increment. The SPA receives the required sequence after long time from the line card, and time out is less in SPA.

  Conditions: Problem is seen when there are more member links in a bundle on SPA-1xCHOC12/DS0 bidirectional traffic is sent. Some bundles drop packets at ingress as lost fragments in one direction.

  Workaround: There is no workaround.

- CSCsw88324

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

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

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

- CSCsw89574

  Symptoms: Under certain circumstances when a route entry containing a repair path is updated or deleted, the repair path may not be properly removed. This may result in the repair path being orphaned in memory consuming a 60 byte memory block.

  Conditions: Occurs with mVPN/TE and multicast enabled on a BGP speaking router. All images based on Cisco IOS Release 12.2(33)SR may be impacted by this problem.

  Workaround: There is no workaround.

- CSCsw89720

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

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

  Workaround: No workaround, other than stopping the query.

- CSCsw89962

  Symptoms: Ping across CE routers fails.

  Conditions: Occurs when “bidir” is configured.

  Workaround: There is no workaround.

- CSCsw90340

  Symptoms: Traffic flows with loopback on a Cisco 7200 router.

Conditions: Occurs when you **shut** the controller, configure loopback, then **no shut** the controller.

Workaround: There is no workaround.

- CSCsw90798

  Symptoms: A Cisco switch may reload after a VLAN is renamed.

  Conditions: Occurred on a Catalyst 6500 running Cisco IOS Release 12.2(33)SXH3a and Cisco IOS Release 12.2(33)SXH4.

  Workaround: There is no workaround.

- CSCsw91320

  Symptoms: A crash occurs with the following footprint:

  ```
  10:08:22 EST Mon Jan 26 2009: Address Error (store) exception, CPU signal 10, PC =
  0x4330E8E0
  0x432DF9F0 ---> dlink_rmqueue+30 0x432DFAEC ---> dlink_dequeue+2C 0x40DF73BC --->
  nrp_service_notification_queue+26C 0x40DF7D8C ---> network_redist_process+210
  ```

  Conditions: Occurs when a multicast protocol is configured on at least one interface. Intermediate System-to-Intermediate System (IS-IS) is configured to run on one of the interfaces on which the multicast protocol is enabled. For example:

  interface TenGigabitEthernet1/1 ip address 10.10.1.21 255.255.255.252 ip router isis ip pim sparse-mode

  IS-IS interface configuration is removed from the interface on which the multicast protocol is configured. If a unicast route owned by IS-IS changes shortly after the multicast interface configuration is removed, the crash may occur.

  Workaround: The following multicast configuration can be used to avoid the risk of a crash:

  ```
  Router(config)#ip multicast rpf multitopology
  Router(config)#global-address-family ipv4 multicast
  Router(config-af)#topology base
  Router(config-af-topology)#use unicast base
  ```

- 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.

- CSCsw92379

  Symptoms: Many “IP ARP: Sticky ARP entry invalidated” syslog messages appear, and the RP reloads unexpectedly.

  Conditions: This symptom is observed when a linecard is swapped while thousands of DHCP snooping bindings are present and the **ip sticky-arp** command is configured.

  Workaround: Configure the **no ip sticky-arp** command.

- CSCsw96484

  Symptoms: An interface that has been error disabled by an OAM remote link failure will not be recovered even if OAM link failure error disable recovery has been configured.

  Conditions: Occurs when Ethernet OAM is configured on the interface and a remote failure is detected.

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

- CSCsw99846

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

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

Workaround: There is no workaround.

- CSCsx05672

  Symptoms: High CPU utilization occurs on the new active supervisor after a stateful switchover (SSO).

  Conditions: Occurs when large numbers of logical interfaces (such as port-channel sub-interfaces or interface VLANs) are configured and earl policing policies applied (uflow policing or aggregate policing) on all the logical interfaces. The CPU utilization on the active supervisor aggravates on each switchover.

  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.

- CSCsx07181

  Symptoms: Router crashes on trying to ping packet over SONET (POS) interface on CHOC12 SPA.

  Conditions: The issue was seen on an internal build based on Cisco IOS Release 12.2(33)SRD. The problem does not occur in the released version of Cisco IOS Release 12.2(33)SRD, but this fix is required to correct an underlying programming error.

  Workaround: There is no workaround.

- CSCsx07317

  Symptoms: Static NAT translations can fail after a reload or crash.

  Conditions: The trigger seems to be a high number of static translations (~100 translations). Once the router is rebooted for any reason, the translations will fail.

  Workaround: Remove and reapply static translations in the configuration.

- CSCsx08294

  Symptoms: A Cisco 6500 running Cisco IOS Release 12.2(33)SXH may encounter a bus error due to OSPF processes.

  Conditions: Occurs when the device is configured for Open Shortest Path First (OSPF).

  Workaround: There is no workaround.

- CSCsx09353

  Symptoms: Switched Port Analyzer (SPAN) is not capturing traffic in both directions. It only captures traffic in one direction.

  Conditions: Occurs when running Cisco IOS Release 12.2(33)SRC or later and with a ES-20 card.

  Workaround: Use another method of packet capture if possible. See VACL capture for details. Removing the SPAN configuration and reapplying it also helps in getting the feature working.

- CSCsx09736

  Symptoms: DHCP failed to get binding under IP as aggregation model with L2 access.

  Conditions: Occurs with IP session with L2 access on a device configured for DHCP relay and VRF transfer.

  Workaround: There is no workaround.

- CSCsx11776

  Symptoms: Executing the commands **show ip bgp version recent 1** or **show ip bgp version 1** from EXEC mode may cause the device to crash.

  Conditions: The symptom is observed in affected images that have support for BGP.

  Workaround: Use AAA command authorization to prevent the use of these commands.

  Further Problem Description: A note regarding BGP Looking Glasses for IPv4/IPv6, Traceroute & BGP Route Servers:

  Per http://www.bgp4.as/looking-glasses, BGP Looking Glass servers are computers on the Internet running one of a variety of publicly available Looking Glass software implementations. A Looking Glass server (or LG server) is accessed remotely for the purpose of viewing routing info. Essentially, the server acts as a limited, read-only portal to routers of whatever organization is running the lg server. Typically, publicly accessible looking glass servers are run by ISPs or NOCs.

  Public Looking Glass servers running an affected version of Cisco IOS are specially susceptible to this bug because they provide unauthenticated public access to Cisco IOS devices. Because of this, operators of BGP Looking Glass servers are encouraged to use AAA to prevent execution of the commands mentioned above that are known to crash Cisco IOS.

- CSCsx15841

  Symptoms: The **BGP aggregate-address** command configured on active RP does not auto-sync to the running configuration of the standby RP.

  Conditions: Occurs when BGP is configured on active/standby redundant RP system.

  Workaround: Configure BGP aggregate-address and reboot the system, forcing both active and standby to load from startup configuration.

- CSCsx17619

  Symptoms: Connectivity between the multilink bundles is lost.

  Conditions: Occurs upon configuration of DLFI over ATM and trying to clear the virtual-access created for multilink using the **clear ppp interface virtual-access<no>** command.

  Workaround: There is no workaround.

- CSCsx18270

  Symptoms: Admin tag is being advertised by the neighbor router. This tag is not showing up in the local router. This causes route filtering based on admin tag to fail.

  Condition: Occurred on a Cisco ASR1000 running Cisco IOS Release 12.2(33)XNB. Other devices and releases of Cisco IOS are affected.

  Workaround: There is no workaround.

- CSCsx20147

  Symptoms: The delay value to destination computed is different between IPv4 and IPv6.

  Conditions: Occurs when EIGRP for IPv6 is configured.

  Workaround: There is no workaround.

- CSCsx20523

  Symptoms: Service-policy is not removed from gigabit interface.

  Conditions: Occurs after you configure a gigabit interface as a switchport and then attach/detach a service-policy.

  Workaround: In order to remove the service policy configuration, go into the mode where the policy was first configured and then unconfigure it.

- CSCsx20566

  Symptoms: Traffic through SIP400 stops or SIP400 displays minor error in **show mod** output.

  Conditions: Seen sometimes on doing RPR+ switchover in a chassis that supports hot fabric synchronization.

  Workaround: Reset the line card.

- CSCsx21231

  Symptoms: SPA-24CHT1-CE-ATM will remain out of service on a SIP-400 because of a missing API.

  Conditions: This issue will be seen during boot up on a Cisco 7600 router with SPA-24CHT1-CE-ATM and SIP-400.

  Workaround: There is no workaround.

- CSCsx21482

  Symptoms: The following commands executed from the console result in a device reload: **write**, **copy running-config startup-config** or **show run**.

  Conditions: The symptom is observed when a large number of interfaces (200+) have been configured for RIPv6 and are active. Interfaces which are down will not contribute to the problem.

  Workaround: There is no workaround.

- CSCsx21606

  Symptoms: On a Cisco 10000 series router that is running Cisco IOS Release 12.2(28)SB11, the serial interface becomes stuck in an up/down state and the multilink interface in a down/down state. The debugs indicate:

  Se7/0/0.10/17:1 PPP: Missed a Link-Up transition, starting PPP Se7/0/0.10/17:1 PPP: Updating buffered PPP packet Se7/0/0.10/17:1 PPP: Starting timer for fast-start Se7/0/0.10/17:1 PPP: Handle allocation failure

  Conditions: The symptom is observed when new T1s are added to the router. The triggers are an SSO configuration and when the router runs for a long time. The new T1s cause a lot of flapping of links.

  Workaround: Reload the router or perform a PRE failover on the Cisco 10000 series router.

- CSCsx22512

  Symptoms: After clearing the DHCP snooping bindings, renewing from the database and reloading the line card, snooping bindings are lost.

  Conditions: Occurs when DHCP snooping is configured to store bindings in the database on the flash disk.

  Workaround: There is no workaround.

- CSCsx23566

  Symptoms: All Layer 3 traffic is silently dropped on the ES40 line card after the module is reset.

Conditions: Occurs when Layer 2- and Layer 3-based Ethernet Virtual Circuits are configured on the ES40. This happens after an RSP fail over or when the module is reset using the **hw-module module # reset** command.

Workaround: Reload the router.

- CSCsx25316

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

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

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

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

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

- CSCsx27659

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

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

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

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

- CSCsx28948

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

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

  Workaround: There is no workaround.

- CSCsx33622

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

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

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

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

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

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

- CSCsx33961

  Symptoms: SNMP engine consumes 100% CPU and device does not respond to SNMP polls.

  Conditions: Occurs when ATM SPA subinterface counters, such as ifInOctets and ifOutOctets are being polled with multiple Varbinds in single SNMP PDU.

  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**.

- CSCsx35306

  Symptoms: Router crashes at “t3e3_ec_safe_start_push”.

  Conditions: The crash is seen immediately after removing the channel-group of the PA-MC-2T3/E3-EC card.

  Workaround: There is no workaround.

- CSCsx37313

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

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

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

- CSCsx37431

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

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

  Workaround: There is no workaround.

- CSCsx39405

  Symptoms: When unconfiguring multicast distribution tree (MDT) and VPN routing/forwarding (VRF), SP crashes.

  Conditions: The problem occurs on scale setup. When number of entries is large on PI multicast side, the PI process can get suspended during delete operation

  Workaround: There is no workaround.

- CSCsx40675

  Symptoms: Router crashes

  Conditions: Occurs during xconnect L2TP session configuration.

  Workaround: There is no workaround.

- CSCsx40747

  Symptoms: A specific configuration of “ip casa” followed by a subsequent use of the command **show running-config** can cause the router to go into an infinite loop and hang.

  Conditions: The symptom is observed when “ip casa” is configured and you enter into config-casa mode. The command **show running-config** will cause the router to hang.

  Workaround: There is no workaround.

  Further Problem Description: This issue is specific to the usage of ip casa. If you do not use casa, you are not vulnerable to the issue described here.

- CSCsx41877

  Symptoms: ATM PVP CLI become inaccessible to the command-line interface.

  Conditions: The commands disappear after configuring l2transport VCs on ATM interface.

  Workaround: Execute default on ATM interface before configuring any L2VC or L2VP.

- CSCsx43897

  Symptoms: CPU utilization goes high when a third session is allowed to be created through SNMP. Also occurs with applications that use SNMP to create sessions, such as NAM GUI.

  Conditions: Perform the SNMPSet on the service module session (this will fail). Now try to create another local session via SNMPSets sequence.

  Workaround: Use CLI to create the sessions.

- CSCsx46858

  Symptoms: Router crashes while configuring MAC addresses.

  Conditions: Occurs when configuring MAC addresses under VT interface in “config-rite” mode.

  Workaround: There is no workaround.

- CSCsx47554

  Symptoms: With a topology like this:

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

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

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

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

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

- CSCsx56369

  Symptoms: Connectivity breaks on SPA based multilink bundles with ACFC/PFC configured when one of the member links go down.

  Conditions: Occurs on a Cisco 7600. Multilink must be SPA based with ACFC/PFC configured. The output of **show ppp multilink** on the RP would show **multilink in hardware**.

  Workaround: Adding back the link or bringing the link back up makes it work.

- CSCsx57465

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

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

  Workaround: There is no workaround.

- CSCsx58268

  Symptoms: The route-map functionality is broken with respect to BGP.

  Conditions: Configure route-map and apply to BGP neighbor as an inbound/outbound policy and then reload the router. The route-map functionality will not work.

  Workaround: There is no workaround.

- CSCsx58369

  Symptoms: DHCP snooping bindings are lost on a Cisco 6724 when online insertion and removal (OIR) is performed on the line card just after renewing the snooping bindings from database.

  Conditions:

  1) Bring up a snooping binding on a Cisco 6724 LC.

  2) Make sure the binding has been written to the snooping database.

  3) Clear the snooping binding by entering the **clear ip dhcp snooping** command.

  4) Write the bindings from the database back to the snooping table by entering the **renew ip dhcp snooping database** command.

  5) Ensure that the binding has been repopulated into the snooping table by entering the **show ip dhcp snooping binding** command.

  6) Perform OIR on the line card.

  7) When the line card comes up, it is seen that the snooping binding is not repopulated. It is lost.

  Workaround: Send a fresh DHCP request from the client.

- CSCsx58889

  Symptoms: Calls fail intermittently with cause “47: no resource available” error.

  Conditions: Occurs when router is under load test.

  Workaround: There is no workaround.

- CSCsx59309

  Symptoms: Cisco IOS routers crash when filter style is changed from fixed filter (FF) to wild card filter (WF).

  Conditions: Occurs when FF style reservation is installed on an interface and is then modified to WF style without first removing the FF style reservation.

  Workaround: Remove FF style reservation before configuring for WF style reservation.

- CSCsx60939

  Symptoms: Standby crashes on deletion of a port-channel.

  Conditions: The problem is seen only when **lacp fast-switchover** is configured on the port-channel.

  Workaround: Shut the port-channel before deleting it.

- CSCsx62080

Symptoms: Cisco ASR crashes into ROMmon when doing DHCP renew from client PC when Cisco Intelligent Services Gateway (ISG) is configured as DHCP relay.

Conditions: Occurs when ISG is acting as DHCP relay and without port-bundle host key (PBHK) enabled.

Workaround: Disable ping using the **ip dhcp ping packets 0** command.

- CSCsx63667

  Symptoms: ES40 line card crashes.

  Conditions:

  1) Have Port-channel with a service instance without encapsulation.

  2) Have members across NPs.

  3) Remove all the members related to 1 NP.

  4) Add a member to the NP, which already has a member.

  5) Line Card crashes.

  Workaround: There is no workaround.

- CSCsx64122

  Symptoms: Service policy disappears from Multilink Frame Relay (MFR) interface.

  Conditions: This is observed after MFR interface flaps.

  Workaround: There is no workaround.

- CSCsx65525

  Symptoms: SIP reloads with the following error messages:

  %C7600_PWR-SP-4-DISABLED: power to module in slot 2 set off (Module Failed SCP dnld)

  %CWAN_RP-6-CARDRELOAD: Module reloaded on slot 2/0

  Conditions: Occurs during switchover from slot6 to slot5 with RSP720.

  Workaround: There is no workaround.

- 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.

- CSCsx76308

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

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

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

  Workaround: There is no workaround.

- CSCsx78074

  Symptoms: Unable to remove ACLs.

  Conditions: Occurs on the ES20. The **no** form of the command does not work.

Workaround: Reload to recover.

- CSCsx78826

  Symptoms: ES20 cards crash due to an address error after a remote Label Distribution Protocol (LDP) session is shut. This is also seen when the remote router is reloaded.

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

  Workaround: There is no workaround.

- CSCsx79111

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

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

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

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

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

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

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

- CSCsx82880

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

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

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

- CSCsx94132

  Symptoms: Router displays the following message:

  SCP-SP-5-ASYNC_WATERMARK: 36152 messages pending in SCP async: LCP#4

  If the number of pending messages keeps increasing, router may eventually crash.

  Conditions: Occurs under the following scenario.

  - With a switchport on ES20 - With more than few hundred allowed VLANs on ES20 trunk - If STP state on the switchports flaps.

  The last condition is critical for the bug to occur.

  Workaround: Prevent conditions leading to STP flaps.

- CSCsx94400

  Symptoms: All traffic through ES line cards stops after a RSP failover. The line cards are powered down and never recover.

  Conditions: Occurs occasionally when a **redundancy force-switchover** is executed on a router containing ES line cards with an N-PE redundancy configuration that looks like the following under a VPLS VFI:

  l2 vfi vfi101 manual

vpn id xxx

forward permit l2protocol all

Workaround: Reload the router. If this does not help, reduce the number of possible core-facing MPLS interfaces that the VPLS pseudowire could possibly take.

- CSCsy01763

  Symptoms: Packets leak from source to destination when PACL is configured and switchover is not complete.

  Conditions: During switchover, and until TCAM is programmed, packets are L3 switched even if the PACL will drop them further. Also, when the PACL is changed, such as addition or removal of ACEs, some packets which are supposed to be dropped will leak to the destination.

  Workaround: There is no workaround.

- CSCsy04594

  Symptoms: When a Cisco 7600 is connected to a different MST region and has a port with root guard configured on the MST boundary port, all VLAN interfaces flap each time a superior BPDU is received on this port. This behavior was observed with Cisco IOS Release 12.2(33)SRB4 and Cisco IOS Release 12.2(18)SXF14.

  Conditions: It was observed in the following context:

  1) The switch is connected to a different MST region 2) It has a port configured as root guard on MST region boundary

  Workaround: Shut down blocked port or remove root guard configuration from the port and the VLAN interfaces stop flapping.

- CSCsy07555

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

  Cisco has released free software updates that address this vulnerability.

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

- CSCsy07830

  Symptoms: All traffic through ES line cards stops after a RSP failover. The line cards fail diagnostics and never recover.

  Conditions: Occurs periodically when a **redundancy force-switchover** is executed on a router containing multiple RSPs and ES line cards.

  Workaround: Reload the router.

- CSCsy08264

  Symptoms: MQC policy applied on ES+ interface may not work as expected. Occurs if too many unique bandwidth rates are configured and applied on same line card and on the interfaces belonging to same Network Processor.

  Conditions: If more than 32 unique bandwidth rates are (defined in policy maps applied on same NP) configured, the policy map is accepted without error but may not work as intended.

  Workaround: If multiple unique bandwidth rates are required, space the policy maps across interfaces based on different network processors.

- CSCsy10610

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

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

Workaround: Disable global VLAN tagging.

- CSCsy17724

  Symptoms: After a reload, CPU on the router remains high and does not recover on its own.

  Conditions: This issue was observed on a reload of a Cisco 7600 router with Supervisor 720. The system had a scaled configuration with a large number of VRF', sub-interfaces and some Virtual Private LAN Services (VPLS) PW. BGP and ISIS routing protocols were also in use. The high CPU is seen in the CEF background process.

  Workaround: An SSO switchover or a system reload can clear the problem.

- CSCsy22193

  Symptoms: After stateful switchover (SSO), adjacency mismatch and traffic failure occur on ES20 sub-interfaces.

  Conditions: This happens when egress QOS/ACL policy is configured on ES20 sub-interface.

  Workaround: Perform a **shut/no shut** on the ES20 interface.

- CSCsy24369

  Symptoms: After removing "priority 30" from policy-map queuing_child, an attempt to add it back fails with the following message:

  Configured Percent results in out of range kbps. Allowed range is 8-622000. The present CIR value is 6.

  Conditions: Occurs with the following configuration:

```
Configure the following policy-map:
Policy Map queuing_child
Class ip_prec_1
priority 30 (%)
Class ip_prec_2
bandwidth remaining 20 (%)
Class ip_prec_3
bandwidth remaining 30 (%)
Class ip_prec_4
bandwidth remaining 49 (%)
Policy Map Dest
Class Dest
Policy Map queuing
Class class-default
Average Rate Traffic Shaping
cir 5000000 (bps)
service-policy queuing_child
```

  Workaround: There is no workaround.

- CSCsy24676

  Symptoms: On occasion, a false positive is returned on a file system failure. File operation is deemed successful when, in fact, it has failed.

  Conditions: This problem occurs when the file system device returns an error and the code follows the path in the file system buffer cache where the error is masked and converted to a success code. This problem is likely to show up if there is a device error during the write. The device error may be due to bad media or an OIR (although it is very unlikely during an OIR).

  Workaround: There is no workaround.

Further Problem Description: This is possible during any file system operation where a file system device is unable to complete the operation and an error is returned. This error is not passed down to the file system stack but is converted to a success code. Other clients which are dependent on previous file system operations fail on successive file system calls and possibly result in a crash.

- CSCsy26370

  Symptoms: Router crashes at af_policer_get_class_drops.

  Conditions: Router crashes while attaching policy under another policy.

  Workaround: There is no workaround.

- CSCsy26526

  Symptoms: Router may reload under excessive **netconf** configuration.

  Conditions: The following configuration commands, when configured repeatedly within a short period of time may cause the device to reload.

  * **netconf ssh**

  * **netconf beep listener**

  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.

- CSCsy28296

  Symptoms: A PPP aggregator may erroneously remove a per-user static route downloaded from RADIUS when the first member link of a multilink group goes down.

  Conditions: Issue observed on Cisco 7200/NPE-G1 running Cisco IOS Release 12.2(33)SRC3 and earlier SRC releases. Also occurs in Cisco IOS Release 12.2(33)SRD.

  Workaround: Clear interface virtual-access (for the MLP bundle). You can also downgrade to Cisco IOS Release 12.2SB.

- CSCsy33145

  Symptoms: Interface default queue traffic is favored instead of the QoS applied to subinterface or EVC traffic.

  Conditions: If there is a mix of QoS policy applied and not applied subinterfaces/EVCs on the main interface, the traffic on the subinterface/EVC without QoS can take the entire physical interface bandwidth, starving the QoS applied subinterface/EVC.

  Workaround: Apply QoS policy on all the subinterface/EVCs on the main interface.

- CSCsy42615

  Symptoms: Entries for ABRs and ASBRs are missing from the OSPF route table. This results in inter-area and external routes being omitted from the Routing Information Base (RIB).

  Conditions: The bug will only be seen when MPLS-TE tunnels are being used. Also, specifying non-default SPF timer values with **timers throttle spf** will increase the risk of hitting this bug.

  Workaround: There is no workaround.

- CSCsy43042

Symptoms: MPLS frames that need to be encapsulated into VRF GRE tunnel are punted to RP if the GRE tunnel requires MPLS imposition.

Conditions: This has been observed on Cisco 7600 provider edge (PE) routers in L3VPN environment.

Workaround: There is no workaround.

- CSCsy45838

  Symptoms: The **show ip ospf border-router** may cause a router to crash.

  Conditions: Occurs if the border table is recalculated in a significant way while the output is being printed on the console. The risk of a crash is reduced if you avoid using the auto-more feature and allow the entire output to display at once.

  Workaround: There is no workaround.

- CSCsy55362

  Symptoms: Console may hang.

  Conditions: Occurs when the TACACS+ server is being used as AAA server and the *single-connection* option is configured.

  Workaround: Remove the single connection option.

- CSCsy55455

  Symptoms: Device running Cisco IOS Release 12.2(33)SRD1 with SAA/SNMP crashes due to bus error.

  Conditions: Occurs when an SNMP poll for IPSLA/SAA values is performed.

  Workaround: There is no workaround.

- CSCsy57786

  Symptoms: The following TOS settings tests fail on ES+ card:

  * TOS mapping from inner to outer IP header via **ip tos reflect** on PW class.

  * TOS setting on outer IP header via **ip tos value** *value*.

  * TOS setting via ingress MQC policy on IP subinterface with **xconnect**.

  Conditions: Occurs on a ES+ card configured for L2TPv3.

  Workaround: There is no workaround.

- CSCsy58886

  Symptoms: Router crash is seen during ISSU with **mls qos** enabled.

  Conditions: Occurs when user does ISSU from Cisco IOS Release 12.2(33)SRC2 to SRC3 or from 12.2(33)SRD1 to later SRD release.

  Workaround: Disable QoS globally using the **no mls qos** command.

- CSCsy75784

  Symptoms: Missing Intermediate System-to-Intermediate System (IS-IS) routes or routing loop occurs after the edge router reloads several times.

  Conditions: Occurs when MT-IPv6 is running and fast convergence parameters are configured.

  Workaround: Enter the **clear isis *** command on the affected router.

- CSCsy81341

Symptoms: When FastEthernet SPA on SIP400 is used as the core-facing side, switch virtual interface (SVI)-based EoMPLS/VPLS traffic does not flow out of the pseudowires. Receiving Traffic on the pseudowire is fine.

Conditions: Occurs when FE spa on SIP400 is used as the core facing side for SVI-based EoMPLS/VPLS. All the imposition traffic is dropped.

Workaround: There is no workaround.

- CSCsy83830

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

  Conditions: Occurs with the following topology

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

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

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

- CSCsy87385

  Symptoms: For IPv6 adjacencies, MTU is incorrectly programmed.

  Conditions: Occurs with simple IPv6/6PE setup.

  Workaround: There is no workaround.

- CSCsy92895

  Symptoms: When SIP-400 is configured as Lawful Intercept service module, after a line card online insertion and removal (OIR), the SIP-400 may not get selected as Lawful Intercept service module.

  Conditions: Occurs when SIP-400 is configured as Lawful Intercept service module on a Cisco 7600.

  Workaround: After line card OIR, select the SIP400 again as the LI service module using the command **li-slot list <sip400 slot number>**.

- CSCsy95540

  Symptoms: L2TP tunnel not coming up for ATM attachment circuit.

  Conditions: The problem is seen on Cisco 7200 router running Cisco IOS Release 12.2(33)SRC.

  Workaround: There is no workaround.

- CSCsz08876

  Symptoms: Packets are not getting in output policy.

  Conditions: Occurs on ES+ card configured for L2TPv3.

  Workaround: There is no workaround.

- CSCsz11877

  Symptoms: MPLS-TE tunnel label reallocation on midpoint router occurs while RSVP is gracefully restarting due to CPU switchover.

  Conditions: Occurs on a Cisco 7600 that is configured as the midpoint router when the upstream node is a Cisco IOS-XR router. This does not happen if the upstream node is also a Cisco IOS router. Because of this label re-allocation, traffic downtime is ~100 msec

Workaround: There is no workaround.

- CSCsz28707

  Symptoms: DHCP binding in DHCP client may not work.

  Conditions: Occurs after online insertion and removal (OIR) operation on a Cisco 7600 with SIP400 line card.

  Workaround: There is no workaround.

- CSCsz29991

  Symptoms: The following error message is displayed:

  %OSPF-4-NULL_PREV_LINKAGE with a traceback of:

  errmsg(0x40636c28)+0x50

  ospf_dlink_delink(0x40eda914)+0x3c

  ospf_service_redist(0x40f2d03c)+0x428

  ospf_router(0x40ee2f20)+0xa24

  This error causes excessive CPU utilization, which causes the Supervisor or RSP to crash.

  Conditions: Occurs after entering the **clear ip ospf process** command, especially in an environment that has multiple OSPF processes. Learning the same prefix with different processes can also cause this condition to occur.

  In this case it was due to the fact that one process was configured with **default-information originate always**, causing an implicit redistribution. The other process was also learning a default route as E2.

  Workaround: To avoid the issue:

  - Clear ip ospf process on a process by process basis few min. apart.

  - Shut/no-shut of the OSPF Process instead of the hard reset/clear

  Reload is the only way to recover if the system has run into the issue already.

- CSCsz42928

  Symptoms: Multicast replicated packets get dropped at “SELENE”.

  Conditions: Occurs when ES+ card is in slot 1 and the port is 1/12.

  Workaround: There is no workaround.

Open Caveats—Cisco IOS Release 12.2(33)SRD1

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(33)SRD1. All the caveats listed in this section are open in Cisco IOS Release 12.2(33)SRD. This section describes only select open caveats.

- CSCsx37608

  Symptoms: Tracebacks observed when **shut/no shut** is performed multiple times on ATM-OC3 interface.

  Conditions: Occurs on a router running Cisco IOS Release 12.2(33)SRD.

  Workaround: There is no workaround.

- CSCsx95984

Symptoms: For C7600 ES+XT Serial line cards, the TenGigaEthernet interface could report erroneous link up status while the link is actually down.

Conditions: This problem is observed with Cisco IOS Release 12.2(33)SRD1. The problem happens when the remote side changes to different transport mode under interface configuration.

Workaround: Every time the remote side changes its transport mode configuration, do a **shutdown** and **no shutdown** for the corresponding interface in the local side.

- CSCsy98323

  Symptoms: Supervisor does not return to SP Prompt after Service line card (SVCLC) tunneling.

  Conditions: After doing a **remote login switch** from supervisor, we go into SUP SP prompt. Then Tunnel into LCP ROMMon through **svclc console** <*slot*> from SUP-sp to boot LCP. Once LCP starts booting, we should come back to SP prompt. This is not happening now.

  Workaround: Type a **^C** to get back to the SP prompt.

Resolved Caveats—Cisco IOS Release 12.2(33)SRD1

Cisco IOS Release 12.2(33)SRD1 is a rebuild release for Cisco IOS Release 12.2(33)SRD. The caveats in this section are resolved in Cisco IOS Release 12.2(33)SRD1 but may be open in previous Cisco IOS releases.

Miscellaneous

- CSCec72958

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

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

  Workaround: There is no workaround.

- CSCec85585

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

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

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

- CSCeg80842

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

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

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

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

- 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**.

- CSCek75694

  Symptoms: A router running Cisco IOS 12.4T may reload unexpectedly

  Conditions: Occurs when BFD is configured and active.

  Workaround: Disable the BFD feature.

- CSCsb98906

  Symptoms: A memory leak may occur in the "BGP Router" process.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(26)S6, that is configured for BGP, and that has the **bgp regexp deterministic** command enabled.

  Workaround: Disable the **bgp regexp deterministic** command.

- CSCse29570

  Symptoms: Router might unexpectedly reload during CNS configuration download.

  Conditions: The downloaded configuration must disable the CNS configuration initial or partial for this crash to occur.

  Workaround: Use static configuration and prevent configuration download from CNS server.

- CSCsg11616

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

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

  Workaround: There is no workaround.

- CSCsg39754

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

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

  Workaround: There is no workaround.

- CSCsh48947

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

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

  Workaround: There is no workaround.

- CSCsi07687

  Symptoms: Self ping to SVI fails when VLAN configurations are removed and reapplied.

  Conditions: Occurs when an interface is deleted and added again.

  Workaround: There is no workaround.

- CSCsi88974

  Symptoms: While configuring a mediation device (MD), if the MediationSrcInterface is set to loopback interface, traffic will cause MALLOC failures.

  Conditions: Problem is seen when traffic rate is equal to or greater than 8000 packets per second.

  Workaround: Do not use loopback0 as MD source interface.

- CSCsj78403

  Symptoms: A router may crash when the **clear ip bgp** command is entered.

  Conditions: Occurs on devices running BGP and configured as a route reflector client with conditional route injection configured.

  Workaround: Unconfigure conditional route injection.

- CSCsk49705

  Symptoms: The **ip nat inside source static network** command does not have the <cr> option.

  Conditions: This symptom is observed on a Cisco 7200 router that is loaded with Cisco IOS Release 12.4 or 12.4T.

  Workaround: There is no workaround.

- CSCsk94179

  Symptom: Connectivity problems are observed for IPv6 client, which obtained IPv6 prefix via DHCP for Virtual Access interface, due to incorrect static routes in the routing table for the assigned IPv6 prefix.

  Conditions: Occurs with IPv6 prefix delegation via DHCP, when client moves from one interface to another.

  Workaround: None

  Further problem description: When IPv6 prefix delegation assigns a prefix for Virtual Access interface, it creates a static route for the prefix in the routing table. When a client moves to a new interface, old binding and the old routes are retained, which causes the problem.

- CSCsl68327

  Symptoms: Packets may be lost during rekey.

  Conditions: Occurs because IPSec transit packets may trigger invalid SPI.

  Workaround: There is no workaround.

- CSCsl71704

  Symptoms: A receive access control list (rACL) with large ACL is not applied on interface if is QoS configured.

  Conditions: Occurs when rACL with large ACL is applied on an interface. It consumes over 60% of ternary content addressable memory (TCAM) space. If the rACL is applied a second interface with QoS, the configuration fails without displaying an error message.

  Workaround: There is no workaround.

- CSCsm28287

Symptoms: After shutting down a GRE tunnel interface, the active RP crashed and switchover took place. The following error message was displayed:

```
%ALIGN-1-FATAL: Illegal access to a low address 13:02:45 UTC Fri Jan 18 2008 addr=0xD,
pc=0x7144A5A0, ra=0x7209FFF8, sp=0x5ABEE90 SLOT0:01:40:03: %DUMPER-3-PROCINFO: pid =
16409: (sbin/ios-base), terminated due to signal SIGBUS, Bus error (Invalid address
alignment) SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: zero at v0 v1
SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: R0 00000000 7A5FD854 EF4321F9
7A6452D0 SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: a0 a1 a2 a3 SLOT0:01:40:03:
%DUMPER-3-REGISTERS_INFO: 16409: R4 EF4321CD 0000000B 0000000B 00000000
SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: t0 t1 t2 t3 SLOT0:01:40:03:
%DUMPER-3-REGISTERS_INFO: 16409: R8 7CB96E10 00FDDBE0 00000000 EFFFFFFF
SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: t4 t5 t6 t7 SLOT0:01:40:03:
%DUMPER-3-REGISTERS_INFO: 16409: R12 00000000 F7E8E12F 00000000 00000000
SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: s0
```

Conditions: Occurred on a Cisco 7200 running an internal build of Cisco IOS Release 12.2SX.

Workaround: There is no workaround.

- CSCsm47417

  Symptoms: W2:setting ceExtSysBootImageList cause **write memory** to work incorrectly.

  Conditions: Occurs after setting ceExtSysBootImageList to a new boot image from SNMP. The new boot image in running-config is not copied to startup-config. Instead, a variable "d" will be copied to startup-config after the **write memory**. The **show bootvar** command will show BOOT variable = d.

  Example:

```
bgl11-lab1-tftp1:/auto/sw/packages/snmpr/15.1.0.3/solaris2bin:3>
bgl11-lab1-tftp1:/auto/sw/packages/snmpr/15.1.0.3/solaris2bin:3>getmany -v2c
10.64.68.138 public ceExtSysBootImageList ceExtSysBootImageList.2001 =
disk1:s72033-adventerprisek9_dbg-vzsm47417test ceExtSysBootImageList.2017 =
disk1:s72033-adventerprisek9_dbg-vzsm47417test
bgl11-lab1-tftp1:/auto/sw/packages/snmpr/15.1.0.3/solaris2bin:4>setany -v2c
10.64.68.138 public ceExtSysBootImageList.2001 -o "disk1:" ceExtSysBootImageList.2001
= disk1: ------------------------------------------------
7600-11-1# 00:02:56: %SYS-5-CONFIG_I: Configured from 10.64.71.240 by snmp
```

  Workaround: There is no workaround.

- CSCsm53196

  Symptoms: Crash occurs at “ip_route_delete_common”.

  Conditions: Occurs under the following scenario:

  1) A multicast BGP route exists.

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

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

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

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

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

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

- CSCsm71537

  Symptoms: The router crashes when Independent Optimized Edge Routing (OER) is configured.

  Conditions: Occurs when OER is configured.

Workaround: There is no workaround.

- CSCsm86832

  Symptoms: The line protocol of the serial interface keeps flapping.

  Conditions: This symptom is observed after BERT is run simultaneously on more than one fractional T1 with a Frame Relay sub-interfaces.

  Workaround: Add and then remove the T1.

- CSCso29361

  Symptoms: The commands given in the **interface range** command may not be synced to all interfaces configured in the range in the standby supervisor.

  Conditions: Occurs when configuration commands are entered under **interface vlan range** command. They get attached to only the first VLAN in the range in the redundant supervisor. After switchover, traffic does not flow due to the missing VLAN configuration.

  Workaround: There is no workaround.

- CSCso40612

  Symptoms: Router is crashing due to random memory corruption in parser code.

  Conditions: The crash happens on only particular sequence and timing of configuration.

  Workaround: There is no workaround.

- CSCso56038

  Symptoms: The following error message may be seen:

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

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

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

  Workaround: There is no workaround.

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

- CSCso57020

  Symptoms: Etherchannel states for Link Aggregate Control Protocol (LACP) port-channels are inconsistent between active and standby, which could possibly affect traffic forwarding.

  Conditions: Occurs while configuring several LACP port channels. This could be seen if LACP port channels are configured and the device is brought up in SSO mode.

  Workaround: Once the standby is completely up in HOT state, perform a **shut/no shut** on the interfaces that are inconsistent.

- CSCso74922

  Symptoms: Resilient Ethernet Protocol (REP) state flaps after line card reset

  Conditions: Occurs on routers running Cisco IOS Release 12.2(33)SRD with SIP600 ports configured as REP edge ports.

  Workaround: There is no workaround.

- CSCso90970

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

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

  Workaround: There is no workaround.

- CSCsq06208

  Symptoms: When health monitoring (HM) diagnostic failure happens, call-home diagnostic messages are not out before platform action is taken.

  Conditions: Call-home is subscribed to diagnostic alert group minor or major error and the gold policy is active. It only happens when the HM diagnostic test interval is small enough.

  Workaround: Set the HM diagnostic test interval to be large enough, but there is no guarantee it will work in all test cases.

  Further Problem Description: Because gold policy is last policy in EEM queue, it waits for call-home messages to send out before it executes. If gold policy continues to trigger on the next test failure after reaching the threshold when action notify flag is already false, it does not need to wait for call-home message to execute. It could crash the system before the call-home message for the last gold policy finishes.

  Adding ACTION_NOTIFY TRUE condition to the gold policy will prevent the gold policy to continuously execute and consistent with call-home message triggering condition.

- CSCsq14261

  Symptoms: Downstream traffic will drop when we send IPv6 traffic over PPPoE sessions.

  Conditions: Bring up a PPPoE session over L2TP tunnel for address negotiated by IPv6, then send downstream IPv6 traffic.

  Workaround: There is no workaround.

- CSCsq42885

  Symptoms: Line card crashes recurrently with the “Address exception error”.

  Conditions: The issue is seen when entering the **no shutdown** command on the spatial reuse protocol (SRP) interface.

  Workaround: There is no workaround.

- CSCsq53542

  Symptoms: After stateful switchover (SSO) there may be loss of multicast packet delivery for 10 or more seconds.

  Conditions: Occurs when multicast routing is enabled in the default mode.

  Workaround: If there are no mStatic or mBGP routes, the following configuration will avoid the problem:

  ```
  Router(config)#ip multicast rpf multitopology
  Router(config)#global-address-family ipv4 multicast
  Router(config-af)#topology base
  Router(config-af-topology)#use unicast base
  Router(config-af-topology)#
  ```

- CSCsq55691

  Symptoms: QoS with Link Fragmentation and Interleaving (LFI) over ATM does not work.

Conditions: Occurs after a **shut/no-shut** on the ATM interface

Workaround: Reload the line card on both ends.

- CSCsq60016

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

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

  Workaround: Break the entry into shorter strings.

- CSCsq77282

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

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

  Workaround: There is no workaround.

- CSCsq77571

  Symptoms: Router (SP) crash may happen upon deleting multiple VRFs or unconfiguring multiple MDTs.

  Conditions: The crash is seen when trying to delete multiple MDTs at one time.

  Workaround: Allow at least seconds after each MDT delete command or VRF delete command before issuing the next command.

- CSCsr05746

  Symptoms: ESM20 line card may crash while booting up.

  Conditions: Occurs intermittently with a scaled topology.

  Workaround: There is no workaround.

- CSCsr09062

  Symptoms: Cisco 7200 crashes due to memory corruption.

  Conditions: Occurs when MLP+QoS is configured on a Cisco 7200 router. QoS policy is having bandwidth, change the BW parameter and flap the multilink using **clear int multilink1** to see the crash.

  Workaround: There is no workaround.

- CSCsr18589

  Symptoms: A Virtual Router Redundancy Protocol (VRRP) group configured on a VLAN interface flaps from the backup to the master state after stateful switchover (SSO) when the existing master is still available on the network. The group will flap back to backup a short period later.

  Conditions: The problem only occurs when there are a large number of VLAN interfaces with a VRRP group configured on each interface and SSO is performed.

  Workaround: Each of the VRRP groups can be configured with a larger VRRP advert timer value. Values should be varied depending on the setup, but a larger than default value is usually required.

- CSCsr18942

  Symptoms: Traceback occurs when VPN routing/forwarding (VRF) is deleted and then recreated.

  Conditions: Occurs when multicast RP is configured under VPN routing/forwarding (VRF) first. When the VRF is deleted, some multicast data may still be locked and not deleted, causing the traceback when a new VRF is created and multicast RP is configured there.

  Workaround: There is no workaround.

- CSCsr26025

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

  Conditions: Occurs under the following scenario:

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

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

  - Failover takes place and RIB is not updated.

  Workaround: There is no workaround.

- CSCsr29468

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

  Cisco has released free software updates that address this vulnerability.

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

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

- CSCsr41079

  Symptoms: Error message seen after stateful switchover (SSO):

  ```
  %CHKPT-4-NOMESSAGE: Message is NULL, (Cannot get data ptr)
  ```

  Conditions: Occurs when Intermediate System-to-Intermediate System (IS-IS) NSF is configured.

  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.

- CSCsr49316

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

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

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

- CSCsr53264

  Symptoms: A software-forced crash occurs on the RP of a Cisco 7600 running Cisco IOS Release 12.2(33)SRB2.

  Conditions: Occurs when the **clear ip route-map***name* command is entered.

  Workaround: Upgrade to Cisco IOS Release 12.2(33)SRC3 or later.

- CSCsr55713

  Symptoms: A crash occurs.

Conditions: The crash is caused by a ping across an ISATAP tunnel. The symptom is observed only in Cisco IOS Release 12.4(15)T7 on the Cisco 7200 (it is not known to affect other platforms), since the crash is dependent on the Cisco IOS memory map (which varies with each image).

Workaround: There is no workaround.

- CSCsr55922

  Symptoms: The EIGRP IPv6 process may incorrectly select a router-ID from the 127.0.0.0 address range.

  Symptoms: The same router-ID may be selected on two separate Cisco routers configured for EIGRP IPv6. External prefixes advertised by one of the EIGRPv6 routers will be ignored by the receiving EIGRPv6 router due to the fact the routerID contained in the external data portion of the prefix matches the receiving routerID; a loop prevention method.

  Workaround:Manually configure a router-ID under the EIGRP IPv6 process with **router-id**<*address*> command.

- CSCsr56465

  Symptoms: Line card MAC notification test fails when redundancy mode is changed from RPR to SSO or SSO to RPR. SIP-400 Bus Connectivity Test failed when the following commands are issued:

  Conf t redundancy mode rpr

  Conditions: The issue observed in the Fabric Hot Sync-enabled Sup720 and RSP720 routers Cisco IOS Release 12.2(33)SRC. In the problem state, Super Santa Ana (SSA) channels are out of sync. For example,**show platform hard ssa status** will display SSA channel status from the SSA based CWAN module console.

  Workaround: There is no workaround.

- CSCsr68497

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

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

  Workaround: There is no workaround.

- 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.

- CSCsr72352

  Symptoms: EBGP-6PE learned IPv6 labeled routes are advertised to IBGP-6PE neighbor by setting NH as local IP address.

  Conditions: This symptom is observed on 6PE Inter-AS Option C with RR case.

  Workaround: There is no workaround.

- CSCsr79367

  Symptoms: Slow synchronization of IP subscriber sessions from Active to Standby RP.

Conditions: This issue is observed only for a large number of IP subscriber sessions. While the traffic is flowing, if user manually requests to clear all the sessions and while that is processing the line card reboots, then standby RP can get into a state there are dangling sessions. This does not render the router useless, but increases the sync time from active to standby.

Workaround: There is no workaround.

- CSCsr80601

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

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

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

- CSCsr81271

  Symptoms: A Cisco 7600 router with PA-A3-T3 port adapter in flexwan module WS-X6582-2PA could generate following error messages with tracebacks upon a mass ATM PVCs flap:

  SLOT 2/0: %CWAN_ATM-3-VC_OR_PORT_ERR: Invalid VCD FF03 or Port: 0 -Traceback= 403E2200 403A8C1C 40344F88 40347FD0 403481B4 403C374C 401CD170

  Slot 2/0 is the slot the port adapter is installed.

  Conditions: This seems to only occur when a large number of ATM PVCs flap, most likely from the service provider side.

  Workaround: There is no workaround.

- CSCsr82785

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

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

  Workaround: There is no workaround.

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

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

- CSCsr84639

  Symptoms: After 30 minutes, MIB synchronization failure messages appear on primary RP. Secondary RP crashes.

  Occurs under the following scenario:

  1) Bringup 1 pppox session on the L2TP network server (LNS)

  2) Pass bidirectional traffic through the LNS

  3) After 30 minutes, MIB sync failures message appear on primary RP and secondary RP crashes.

  Workaround: Enter the **no snmp mib notification-log default** command.

- CSCsr86515

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

%SYS-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs (129/17),process = Virtual Exec. -Traceback= 40B5D8A8 40B5D984 40B5DA4C 40B5DB78 40B5DC6C 40C0E1BC 4125D3A8 4209FAEC 420AA5A0 4054C05C 420570D8 40575510 41257298 41257284
%SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Virtual Exec. -Traceback= 40B5D8C8 40B5D984 40B5DA4C 40B5DB78 40B5DC6C 40C0E1BC 4125D3A8 4209FAEC 420AA5A0 4054C05C 420570D8 40575510 41257298 41257284

Conditions: This was observered on a Cisco 7600 with Supervisor 720 running Cisco IOS Release 12.2(33)SRB3 after a ATM sub-interface was removed.

Workaround: There is no workaround.

- CSCsr86826

  Symptoms: A standby SP may experience a memory leak in the mls-hal-agent process.

  Conditions: This has been experienced on a Cisco 7600 router with dual SUP720s running either Cisco IOS Release 12.2(33)SRC or Cisco IOS Release 12.2(33) SRC1. The router is configured for multicast.

  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.

- CSCsr97343

  Symptoms: An MSDP peer may flap randomly.

  Conditions: The symptom is observed when the device is configured with **logging host** *ip-address ...* or **logging host** *ip-address*.

  Workaround: It has been observed that removing the "logging host" configuration helps in preventing the peer-flap: **no logging host** *ip-address* **no logging** *ip-address*

- CSCsr97753

  Symptoms: Pinging an interface fails.

  Conditions: Occurs when unconfiguring xconnect on the interface.

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

- CSCsr98731

  Symptoms: If running OSPF, stale routes may be installed in the RIB. Also wrong paths (inter-area vs intra-area) are preferred.

  Conditions: Occurs on a router running Cisco IOS Release 12.2(33)SRC1.

  Workaround: There is no workaround.

- CSCsu04088

  Symptoms: With unidirectional Ethernet (UDE) enabled on ES20 port, UniDirectional Link Detection (UDLD) gets disabled. But on converting the port from L3 to L2 (or vice versa) or on shut/no shut of interface, UDLD is enabled again on the interface. Once UDLD gets enabled, due to the UDE feature, the port is detected as unidirectional and put to err-disabled state.

  Conditions: Occurs on ES20 ports configured for both UDE and UDLD.

  Workaround: Disable UDLD on the port.

- 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.

- CSCsu04473

  Symptoms: Upon the first SSO switchover triggered with the **redundancy force-switchover** command, the traffic stops on the ATM N-to-1 VCC pseudowires configured with cell-packing in the direction from the MWR towards the 7600 SPA-4XOC3-ATM interface. Traffic recovers normally in the other direction.

  Conditions: Occurs on a Cisco 7600 S-series equipped with dual SUP720-3BXL. The problem is seen only when cell-packing is enabled on the N-to-1 VCC pseudowires and when APS (MR-APS) is configured on the ATM OC3 interface of the Cisco 7600 SPA-4XOC3-ATM.

  Workaround: Disable cell-packing on the ATM N-to-1 VCC pseudowires or alternatively disable APS on the SPA-4XOC3-ATM interface.

- CSCsu05525

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

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

  Workaround: Clear the session to remove the configuration.

- CSCsu08935

  Symptoms: BGP as-override does not work properly on a PE to overwrite the AS in the AS4_PATH.

  Conditions: When a 4 byte CE is peered to a 2 byte capable PE using AS 23456 and the command **as-override** is configured on the neighbor, the PE router does not override the AS in the AS4_PATH with its own AS number, mapped to 4 bytes.

  Workaround: Use "allowas-in" on the CE.

- CSCsu10229

  Symptoms: cdpCacheAddress(OID:1.3.6.1.4.1.9.9.23.1.2.1.1.4) MIB is not showing GLOBAL_UNICAST address.

  Conditions: Occurs on a Cisco 7200 router running Cisco IOS Release 12.4(15)T7.

  Workaround: There is no workaround.

- CSCsu12040

  Symptoms: BGP neighbors that are configured with as-override and send-label (CsC) together may not work after an interface flap or service reset.

  Conditions:

  neighbor xxx as-override neighbor xxx send-label

  Workaround: Enter the "clear ip bgp * soft in" command.

  Further Problem Description: Peers (neighbors) with a CsC (IPv4+label) BGP configuration with the as-override option should be separated into different dynamic update groups during the BGP update generation process. After the CSCef70161 fix in Cisco IOS Release 12.0(32)SY4, this is no longer the case; this CSCsu12040 fix enhances the CSCef70161 fix to handle the CsC (IPv4+label) case separately.

- CSCsu24087

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

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

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

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

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

- CSCsu27109

  Symptoms: When stateful switchover (SSO) is performed on a Cisco 7600, MPLS label allocation fails.

  Conditions: Issues are seen on Cisco 7600 router. Occurs after performing the SSO. Also seeing CPU usage above 95% for 10-15 minutes.

  Workaround: There is no workaround.

- 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.

- CSCsu27894

  Symptoms: Flurry of DUP_IFINDEX messages are seen on standby.

  Conditions: Occurs during bulk sync phase when standby is coming up.

  Workaround: There is no workaround.

- CSCsu31088

  Symptoms: Not able to execute any commands under interface after running BERT tests.

  Conditions: This issue is seen only after running SPA FPGA BERT tests and also when there is dual RP in chassis. With other BERT options, no issue is seen.

  Workaround: There is no workaround.

- CSCsu31935

  Symptoms: Bootup diag test failures observed on 6816 card when multirouters are reloaded. Some ports were put in error disabled state.

  Conditions: Failure trigerred with random multirouters reloads (reload of CE1, PE1, Core1). Brief router info and config: IOS - 8/25 a76 Dual sup720 7606 6724 connected to remote 6724 (servicing vlans 2-2000) 6816 connected to remote 6816 (servicing vlans 2001-4000) sip600 (servicing vlans 1-4000 switchport)

  Topology:

  CE1----PE1----Core-1-----Core-2----PE2----CE2 Affected router is CE1.

  Configuration: 4k VLANs, 6816 servicing VLANs 2001-4000 (switchports).

  Workaround: Run the failing diag tests on demand.

Further Problem Description: Few bootup tests fail when on 6816 card when the multirouters are reloaded. On failure, the ports are put in error disabled state. Failure cause has been root caused to usage of reserved diag vlans in the configs. Please refer the link mentioned below.

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.1E/native/command/reference/S1.html

switchport dot1q: Do not enable the reserved VLAN range (1006 to 1024) on trunks when connecting a Catalyst 6500 series switch running Cisco IOS software on both the supervisor engine and the MSFC to a Catalyst 6500 series switch running Catalyst software. These VLANs are reserved in systems running Catalyst software. If enabled, systems running Catalyst software may error disable the ports if there is a trunking channel between these systems

When the diag vlans (1006 to 1011, 4094 to 4089) are used, there could be diag failures at some random cases. Please do not enable the reserved vlans.

- CSCsu31954

  Symptoms: A router reloads.

  Conditions: Under certain crypto configurations with NetFlow also configured, the router will reload when required to fragment CEF-switched traffic on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsu35597

  Symptoms: Renaming a directory gives error message.

  Conditions: This happens on a Cisco router running Cisco IOS Release 12.4(20)T1.fc2 image

  Workaround: There is no workaround.

- CSCsu35624

  Symptoms: When a private VLAN is configured on a VTPv3 server and then deleted, the update message on a peer VTPv3 client can cause a stack overflow for VLAN manager process and crash.

  Conditions: Occurs in a Cisco 7600 running Cisco IOS Release 12.2(33)SRD.

  Workaround: There is no workaround.

- CSCsu36697

  Symptoms: The line card reloads when a line card online insertion and removal (OIR) is performed. It does not happen consistently.

  Conditions: This occurs when an empty policy is present.

  Workaround: There is no workaround.

- CSCsu36709

  Symptoms: A router may unexpectedly reload.

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

  Workaround: Do not use EIGRP to redistribute BGP.

- CSCsu37205

  Symptoms: BGP dampening under VPNv4 may cause router crash.

  Conditions: Occurs when BGP dampening is enabled on VPNv4 address family, but not on individual **IPv4 VRF**<*VRF-name*>**address-family**.

Workaround: Enable the same set of BGP dampening on both the VPNv4 address family as well as all entries for IPv4 VRF address-family.

- CSCsu39152

  Symptoms: IF-MIB registration fails as there are no free ifIndex available.

  Conditions: Occurs after an upgrade. Seen only in HA systems.

  Workaround: There is no workaround.

- CSCsu39704

  Symptoms: Unable to configure pseudowire on virtual-PPP interface. Command is rejected with the following error:

  Incompatible with ip address command on Vp1 - command rejected

  Conditions: Occurs when IPv4 address or IP VPN routing/forwarding (VRF) has already been configured on the main interface.

  Workaround: There is no workaround.

- CSCsu40667

  Symptoms: A Cisco 7600 series router may fail to install some NetFlow entries even if NetFlow table utilization is low.

  Conditions: Occurs while flows are ingressing on ES20 module.

  Workaround: There is no workaround.

  Further Problem Description: The **show mls netflow table-contention detail** command will show a heavy ICAM table utilization, while TCAM utilization is small.

  Router#**sh mls net table-contention det**

  Earl in Module 1

  Detailed Netflow CAM (TCAM and ICAM) Utilization

  ==========

  TCAM Utilization : 0%

  ICAM Utilization : 98%

  Netflow TCAM count : 152

  Netflow ICAM count : 126

  Netflow Creation Failures : 388663

  Netflow CAM aliases : 0

- CSCsu42315

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

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

  Workaround: There is no workaround.

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

- CSCsu44992

Symptoms: VPDN redirect functionality does not work.

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

Workaround: There is no workaround.

- CSCsu46822

  Symptoms: When account logon is done for a DHCP user, QoS policies defined in the user profile are not applied to the ISG session.

  Conditions: A DHCP session is created. User performs account logon via SESM (not CoA). User profile has QoS polices defined. Session is authenticated but policies are not applied to the session.

  Workaround: Perform account logon using CoA.

- CSCsu46871

  Symptoms: Unable to attach service policy to VT when bandwidth is configured in class default.

  Conditions: Occurs when DLFI over ATM is configured while trying to attach service policy to VT when bandwidth is configured in class default.

  Workaround: Configure bandwidth in user defined class and attach to VT.

- CSCsu47037

  Symptoms: Router crashes when an attempt is made to forward a packet out of an Auto-Template interface.

  Conditions: This occurs when the interface's MTU is set to 0: Use the **show interface Auto-Template X** command to show the MTU.

  Workaround: Configure a protocol MTU directly on the Auto-Template interface.

- CSCsu48898

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

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

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

- CSCsu50118

  Symptoms: More convergence time seen even with the **carrier-delay msec 0** command configured.

  Conditions: Occurs when **carrier-delay msec 0** is configured on a gigabit interface.

  Workaround: If excessive convergence time is observed even with the **carrier-delay msec 0** command configured, enter the command again on the interface.

- CSCsu51095

  Symptoms: If connected routes are optimized using PfR, there will be a routing loop.

  Conditions: This symptom can occur if, for some reason, PfR is learning connected routes or if the user has configured them.

  Workaround: Create an oer-map with a prefix-list that contains the prefixes with the IP addresses of the connected routes (the next hops). Set the set observe mode in the oer-map.

- CSCsu51245

  Symptoms: Port-channel QinQ subinterface on ESM20 and SIP600 line cards do not pass traffic after router reload and line card reset.

  Conditions: This condition is seen after router reload or member link line card reset. This is not seen when configuration is newly applied.

Workaround: To recover from the condition, perform a **shut/no shut** on the port channel main interface.

- CSCsu54801

  Symptoms: IPv6/IPv6 Tunnel adjacency information is incomplete on the line card. This prevents IPv6/IPv6 multicast traffic on the tunnel.

  Conditions: The symptoms are observed under normal operation.

  Workaround: There is no workaround.

- CSCsu55145

  Symptoms: Router crashes due to critical software exception.

  Conditions: Occurs on a Cisco ASR 1000 running Cisco IOS Release 12.2.

  Workaround: There is no workaround.

- CSCsu55883

  Symptoms: With MLPPP configured on OSM, the following symptoms may be observed:

  1. Line card might crash.

  2. Links might flap.

  3. Following error message from line card might be seen: "SLOT 9: Sep 14 13:48:48.479 CDT: %COMMON_FIB-3-FIBIDBINCONS2: An internal software error occurred. Multilink1 linked to wrong idb R11_Mu1"

  Conditions: Occurs on routers running various Cisco IOS Release 12.2SR releases. Performing a **shut/no shut** on the OSM (especially on the card containing MLPPP) interfaces might trigger this issue.

  Workaround: There is no workaround.

- CSCsu57331

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

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

  Workaround: Reset the line card.

- CSCsu57958

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

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

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

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

- CSCsu62667

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

Conditions: Occurs following a SSO switchover.

Workaround: There is no workaround.

- CSCsu63996

  Symptoms: NSF restart may be terminated and OSPF NBR may flap during RP switchover. The **debug ip ospf adj** command shows the following message: OSPF: Bad request received.

  Conditions: The symptoms are observed when the links are broadcast networks and the restarting router is DR. It is seen when "nsf cisco" is configured and when some neighbors finish OOB resync much sooner than others.

  Workaround: Use the **nsf ietf** command.

  Alternate workaround: Configure routers so that the restarting router is not DR (use ospf network type point-to-point or priority 0).

- CSCsu64215

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

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

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

- CSCsu65189

  Symptoms: If router is configured as follows:

  router ospf 1 ... passive-interface Loopback0

  And later is enabled LDP/IGP synchronization using command

  Router(config)#router ospf 1 Router(config-router)# mpls ldp sync Router(config-router)#^Z

  MPLS LDP/IGP synchronization will be allowed on interface loopback too.

  Router#sh ip ospf mpls ldp in Loopback0 Process ID 1, Area 0 LDP is not configured through LDP autoconfig LDP-IGP Synchronization : Required < ---- NOK Holddown timer is not configured Interface is up

  If the **clear ip ospf proc** command is entered, LDP will keep the interface down. Down interface is not included in the router LSA, therefore IP address configured on loopback is not propagated. If some application like BGP or LDP use the loopback IP address for the communication, application will go down too.

  Conditions: Occurs when interface configured as passive. Note: all interface types configured as passive are affected, not only loopbacks.

  Workaround: Do not configure passive loopback under OSPF. Problem only occurs during reconfiguration.

  The problem will not occur if LDP/IGP sync is already in place and: - router is reloaded with image with fix for CSCsk48227 - passive-interface command is removed/added

- CSCsu65225

  Symptoms: TFTP from supervisor to ACE modules fail.

  Conditions: Results in the inability to copy/upgrade images to standby ACE. This is due to moving all 127.x.x.x addresses in an internal VPN routing/forwarding (VRF), which causes TFTP to fail.

Workaround: ACE modules could fail-over to make standby as active and then ftp from the server directly.

- CSCsu67461

  Symptoms: Router may crash when "show tracking brief" is entered if one or more tracking object have been created using the Hot Standby Routing Protocol (HSRP) cli, such as **standby 1 track Ethernet1/0**.

  Conditions: This does not occur if all tracking objects use the new **track** command as follows:

  track 1 interface Ethernet1/0 line-protocol interface Ethernet 0/0 standby 1 track 1

  Workaround: Use **show tracking** instead, or configure tracking with the new command.

- CSCsu67637

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

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

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

- CSCsu69590

  Symptoms: After Flex Link failover, connectivity may be lost. Configured VLANs might be pruned on active link, causing VLAN interface to go down.

  Conditions: This usually happens after the second Flex Link failover.

  Workaround: Remove the Flex Link configuration from the interface, then reconfigure it.

- CSCsu71728

  Symptoms: A crash may occur while applying QOS under an MFR interface.

  Conditions: The symptoms are observed while applying QOS under an MFR interface on a PA-MC-2T3-EC in L2VPN.

  Workaround: There is no workaround.

- CSCsu72025

  Symptoms: SIP400 may crash during Change of Authorization (CoA) push.

  Conditions: Occurs on a SIP400 with ACL configurations on iEdge sessions and CoA push enabled.

  Workaround: There is no workaround.

- CSCsu74397

  Symptoms: When removing PA-MC-8TE1+ from the chassis, the router has an unexpected system reload. This reload happens when you remove the port adapter and the router is running the Cisco IOS bootloader image. Also happens when the port adapter is removed after the router finishes loading the Cisco IOS bootloader image and before it loads the complete Cisco IOS Software image.

  Conditions: This occurs on a Cisco 7200 VXR NPE-G2 Series Routers on the Cisco IOS bootloader image from the Cisco IOS Release 12.4(4)XD.

  Workaround: Remove PA-MC-8TE1+ when the complete Cisco IOS Software Image finishes loading.

- CSCsu77549

Symptoms: Protocol Independent Multicast (PIM) VPN routing/forwarding (VRF) neighbors not formed.

Conditions: Occurs after line card reload.

Workaround: Delete and add back the MVPN configuration.

- CSCsu78559

  Symptoms: In scaled conditions (8000 IP sessions) with SACL applied, line card memory leaks over a period of 4-5 hours. Sometimes this even results in a line card crash. The "Sacl Np Client" task occupies most of the CPU, and a large number of IP sessions (around 10% of 8k) will be in feature pending status, with ACL pending flag set.

  Conditions: Occurs under scaled conditions with approximately 8000 IP sessions, with the same SACL applied to all IP sessions.

  Workaround: There is no workaround.

- CSCsu79340

  Symptoms: Cisco router crashed while Intermediate System-to-Intermediate System (IS-IS) is coming up.

  Conditions: Occurred only on a Cisco router running Cisco IOS Release 12.2(33)SRC2 with ’mpls traffic-eng multicast-intact’ configured under ’router isis’.

  Workaround: disable ’mpls traffic-eng multicast-intact’ configuration.

- CSCsu81406

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

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

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

- CSCsu82893

  Symptoms: Features requiring nas-port as a username determined by AAA (such as pre-auth) will not work on the standby device, causing standby sessions to be poisoned.

  Conditions: AAA calculates the IP address of the best port, which is up and active. However, on the standby device, no interface is visibly active, resulting in a best IP address defining the router to be 0.0.0.0.

  Workaround: There is no workaround.

- CSCsu83563

  Symptoms: Multicast rate-limiters stop working after a HA switchover.

  Conditions: To see this issue you have to have a HA setup with multicast rate-limiters set. In order to see this issue the rate-limiters must have been set before the standby is booted. If the rate-limiters are set after standby is up in HOT state, the issue is not seen after switchover.

  Workaround: Remove and reconfigure the rate-limiters.

- CSCsu83588

  Symptoms: After a router reload, the Flex Link configuration (**switchport backup interface Po#**) is lost.

  Conditions: Occurs when a backup interface is a port-channel interface.

  Workaround: There is no workaround.

- CSCsu87248

Symptoms: Router crashes while adding flexible NetFlow.

Conditions: Occurred on a router running Cisco IOS Release 12.2(33)SRC1.

Workaround: There is no workaround.

- CSCsu88256

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

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

  Workaround: There is no workaround.

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

- CSCsu89550

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

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

  Workaround: Remove the control-plane policy.

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

- CSCsu90280

  Symptoms: IPv6 DMVPN tunnel does not work. IPv6 NHRP registration between Hub and Spoke fails.

  Conditions: The symptoms are observed under normal operation.

  Workaround: There is no workaround.

- CSCsu92966

  Symptoms: Send statistics from the **show mpls l2 vc** command are not displayed.

  Conditions: Occurs on a PE when the other PE's core-facing link is flapped.

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

- CSCsu93374

  Symptoms: The group state of a slave group may unexpectedly change to Active after an RP switchover.

  Conditions: The symptom is observed when HSRP multigroup is configured such that a slave group follows the state of a master group. If the HSRP group state is Standby, then the group state of the slave group may change to Active after an RP switchover.

  Workaround: There is no workaround.

- CSCsu94030

  Symptoms: Internal VRF gets disabled at when the router boots up.

  Conditions: Occurs after any failover or router start-up scenario

  Workaround: Use the **no platform ivrf disable** to avoid the issue.

- CSCsu94720

  Symptoms: Router crashes when the **shutdown** command is used on an interface.

  Conditions: Occurs when there are DHCPv6 bindings.

  Workaround: There is no workaround.

- CSCsu94864

  Symptoms: The MLS shortcut for a user-traffic flow based on RADIUS Framed-IP (FIP) is not purged when the FIP sticky times out. RADIUS Load Balancing (RLB) sends out a purge request before deleting sticky and has no effect in deleting the MLS shortcut entry.

  Conditions: Occurs on a device configured with RLB and FIP sticky idle timer and with MLS aging timer configured higher than the RLB FIP sticky idle timer.

  Workaround: There is no workaround.

- CSCsu96649

  Symptoms: On Cisco 7600 with RSP720-3C-10GE processor, if the SIP-400 is configured as Lawful Intercept (LI) service module after a line card online insertion and removal (OIR), the SIP-400 may not get selected as Lawful Intercept service module.

  Conditions: Occurs when the SIP-400 is configured as Lawful Intercept service module on the Cisco 7600.

  Workaround: After line card OIR, select the SIP-400 again as the LI service module using the command **li-slot list** <*sip400 slot number*>.

- CSCsu96730

  Symptoms: Intelligent Services Gateway (ISG) traffic from one user to another may fail if the packet needs to be processed by the RP in a Cisco 7600.

  Conditions: Occurs when ISG is configured and packets are switched from one subscriber to a second subscriber.

  Other symptoms : - Counters of packet transfer might show difference between user transferring between each other - Access-list might fail to block the packet

  The 2 above symptoms will be seen when user are sending receiving on the same interface via the ISG

  Workaround: There is no workaround.

- CSCsv00168

  Symptoms: Junk values are being displayed on the router when characters/commands are inputted. For example, enter "enable", it shows "na^@^@"; enter "show version", it shows "h ^v^@e^@^r^@^@^@^@^@".

  Conditions: The symptoms are observed with Cisco IOS Release 12.4(23.2)T.

  Workaround: There is no workaround.

  Further Problem Description: The CLI function is not affected by the junk values.

- CSCsv03300

  Symptoms: Cisco 7200 NPEG2 router crashes while displaying the interface output for onboard gigabit ethernet using the **show interface gig0/x** command.

  Conditions: Occurs when a CBWFQ QoS policy is attached to the onboard gigabitethernet interface.

  Workaround: There is no workaround.

- CSCsv04674

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

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

Workaround: There is no workaround.

- CSCsv04836

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

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

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

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

- CSCsv05934

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

  Workarounds: There are no workarounds available for this vulnerability.

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

- CSCsv06608

  Symptoms: SXP is set up between two devices but fails to initialize.

  Conditions: This symptom is observed when SXP is set up between two devices.

  Workaround: There is no workaround.

- 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.

- CSCsv08528

  Symptoms: After the Resilient Ethernet Protocol (REP) topology is returned by the **rep preempt** command, MAC address table is not cleared.

  Conditions: During internal testing, this occurred approximately 3 times out of 20.

  Workaround: Use the **clear mac-address-table dynamic** command to clear the table.

- CSCsv13243

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

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

Workaround: Configure subinterface in "non-native" mode.

- CSCsv13738

  Symptoms: There are two ways to define VRFs when supporting the 6VPE feature: 1) ip vrf 2) vrf definition. The "vrf definition" configuration may take a much longer time to allow convergence between the PE and the CE than the "ip vrf" configuration.

  Conditions: The symptoms are observed under the following conditions: - when the router boots up; and - when the issue has been seen using the "vrf definition" configuration; and - when the router has over 100,000 VPNv4 BGP routes; and - when a large number of VRFs are configured.

  Workaround: Use the "ip vrf" configuration, if you have only IPv4 VRFs configured.

- CSCsv13914

  Symptoms: Traceback observed when the PPPoEoA session is brought up.

  Condition: Occurs when the interface is not up.

  Workaround: There is no workaround.

- CSCsv15040

  Symptoms: Infinite Loop occurs when doing MIB walk on cdot1agStackTable objects.

  Conditions: Occurs on a Cisco 7600 running Cisco IOS Release 12.2(33)SRD and configured with 10GE-XFP-SPA and SIP-600 configured for Distributed Forward. This problem is seen when "MIP/MEP" configured on Te1/0/0 interface and MIB walk is performed on cdotagStackTable objects.

  Workaround: Do not configure "MIP/MEP" on Te1/0/0 interface.

- CSCsv16869

  Symptoms: BGP updates may not be sent out.

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

  Workaround: There is no workaround.

- CSCsv20125

  Symptoms: PPPoE sessions over VLAN over ATM with process switch stuck at LCP stage.

  Conditions: Occurs when the **protocol pppovlan** command is configured on ATM subinterface along with **no ip cef**. PPPoE sessions are not created.

  Workaround: Use the **ip cef** command.

- CSCsv21295

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

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

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

- CSCsv21403

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

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

  Workaround: There is no workaround.

- CSCsv22930

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

  Conditions: Occurs when pseudowire stitching is configured.

  Workaround: Do not enable FRR between these routers.

- CSCsv23252

  Symptoms: A Cisco 7600 running Virtual Private LAN Services (VPLS) with QinQ tunnels is forwarding CDP/VTP packets from the tunnel interfaces across remote sites, even when L2TP is not enabled.

  Conditions: Occurs with a VPLS setup with QinQ tunnel interfaces facing the customer edge.

  Workaround: Use different domain names to avoid changes to VTP database.

- CSCsv24179

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

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

  Workaround: There is no workaround.

- CSCsv24908

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

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

  Workaround: Reload the chassis.

- CSCsv25306

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

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

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

- CSCsv27428

  Symptoms: TCP sessions passing through a NAT router freeze.

  Conditions: The NAT router is a Cisco 7600 with RSP720. NAT translation entries keep using syn-timeout (default = 60 sec) even after TCP three-way handshake is done. Use **show ip nat translation verbose** to check timer

  Workaround: Use the **ip nat translation syn-timeout** command, which mitigates the problem to some extent.

- CSCsv27617

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

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

Workaround: Remove and reconfigure NetFlow on the affected interfaces.

- CSCsv30307

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

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

  Workaround: There is no workaround.

- CSCsv30540

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

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

  Workaround: There is no workaround.

- CSCsv33977

  Symptoms: BGP peer fails to exchange the OPEN Message for negotiating capability when the neighbor router does not support any BGP capabilities.

  Conditions: The symptom is observed when the neighbor router does not support any BGP capabilities and when the capability negotiation fails due to an SSO switchover.

  Workaround: Configure "neighbor x.x.x.x dont-capability-negotiate". Issue the **clear ip bgp *** command when the issue occurs.

- CSCsv35120

  Symptoms: The ES20-GE3C/GE3CXL line card may crash if the explicit-path of an MPLS Traffic Engineering (TE) tunnel is changed so that it no longer goes out a core-facing port-channel interface.

  Conditions: Seen only when the following conditions are met:

  - Virtual Private LAN Services (VPLS) traffic passes over the MPLS Traffic Engineering tunnel.

  - Traffic going out the tunnel initially goes over a port-channel interface.

  - Five or more ports on the ES20 line card are used in the port-channel interface.

  - The explicit-path specified avoids the port-channel interface

  Workaround: Shut down the port-channel interface first before changing the tunnel’s explicit-path.

- CSCsv38166

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

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

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

  Cisco has released free software updates that address this vulnerability.

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

This advisory is posted at the following link:

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

- CSCsv41886

  Symptoms: Entering the **no ip routing** or **no router bgp xx** command yields the following error message:

  %IPRT-3-IPDB_DEL_ERROR: i_pdb delete error bgp, 4, 210074C8, 20E322E0, 0, 0 -Process= "IP RIB Update", ipl= 0, pid= 117, -Traceback= 0x61FD7F58 0x62005498 0x62006D24

  Conditions: Occurs when a large number of VRFs must be configured and BGP is also configured to support these VRFs, then a **show** command, such as **show run**, is issued shortly after the **no ip routing** or **no router bgp** command.

  Workaround: There is no workaround.

- CSCsv42176

  Symptoms: Router reloads, and the following error is displayed:

  SP: MACSEC: Assert failure: mat_rc >= BD_MAT_RET_SUCCESS

  Conditions: Occurs when, for a given service instance, a secure entry is removed with **mac security aging** *inactivity* configured and **mac security** configured.

  This can occur through the CLI via a command like **clear ethernet service instance id** *id interface interface id* mac table, or it can occur due to EFP shutdown.

  If this occurs at the same time that the entry's aging timer expires, the reload may occur.

  <B>Workaround:</B>

  There is no workaround if "aging inactivity" is required. This problem will not occur if **mac security aging** *inactivity* is not configured.

- CSCsv50159

  Symptoms: Spurious access or crash seen on a router with a CEoP SPA, when bulk sync happens between RP and RPR.

  Conditions: Occurs duing regular bootup.

  Workaround: There is no workaround.

- CSCsv59031

  Symptoms: SIP-400 crashes on RADIUS CoA push with Cisco Intelligent Services Gateway (ISG).

  Conditions: Occurs on a SIP-400 configured for IP/PPPoE sessions and ACL configuration push from other router.

  Workaround: There is no workaround.

- CSCsv66827

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

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

  Workaround: There is no workaround.

- CSCsv73388

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

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

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

- CSCsv73735

  Symptoms: After performing a redundancy switchover (RPR+ mode), the ARP table is not correctly populated. Entering the **clear ip arp** or the **clear arp-cache** commands, then pinging the connected CE or PE causes an incomplete entry to be added to the ARP table.

  Conditions: This is seen on Gigabit Ethernet, FastEthernet and POS interfaces. ATM and serial interfaces seem do not appear to be affected. This behavior is not seen with stateful switchover (SSO).

  Workaround: There is no workaround.

- CSCsv79993

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

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

  router eigrp 10

  network 10.0.0.0

  distribute-list 49 out Ethernet1/2.10

  router rip

  network 10.0.0.0

  default-metric 2

  distribute-list 49 out Ethernet1/2.10

  Workaround: There is no workaround.

- CSCsv81009

  Symptoms: Intermittent traffic loss occurs on switch virtual interface (SVI) enabled with Virtual Router Redundancy Protocol (VRRP). Cannot ping VRRP IP address.

  Conditions: Occurs with VRRP configured on SVI. Traffic loss/ping VRRP IP address failure seen sometimes on bootup.

  Workaround: If VRRP mac-address is present as dynamic entry on bootup, this issue can be seen. Reconfigure VRRP as a workaround.

- CSCsv85990

  Symptoms: If there are multiple EFPs with, for example encapsulation 100, same encapsulation on different interfaces and with different bridge-domains configured for Virtual Private LAN Services (VPLS), then if there is a topology change notification (TCN) received on one of the Ethernet Flow Points (EFPs) on one interface, then Label Distribution Protocol (LDP) MAC address withdrawals are sent for all the bridge domains on all the interfaces.

  Conditions: Occurs when the network has EVCs on the L2-Access forwarding to VPLS core. Multiple Spanning Tree (MST) is running on the access VLANs.

  Workaround: There is no workaround.

- CSCsv86256

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

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

  Workaround: Disable FRR at the stitching point.

- CSCsv86288

  Symptoms: Sending a NETCONF hello reply which contains a "session-id" element triggers an instant crash. The device will report a reload due to a bus error.

  Conditions: This occurs when sending a hello reply which contains a session-id element. A hello without this element, one which only contains NETCONF capabilities, does not cause a crash.

  Workaround: Send a NETCONF hello without a session-id element.

- CSCsv90323

  Symptoms: ISSU upgrade to Cisco IOS Release 12.2(33)SRD did not put router into route processor redundancy (RPR) mode.

  Conditions: Occurs when **no service image-version efsu** is enabled. During ISSU upgrade from Cisco IOS Release 12.2(33)SRB or SRC to Cisco IOS Release 12.2(33)SRD, the router incorrectly goes into stateful switchover (SSO). The correct mode is RPR because SSO ISSU from these releases to Cisco IOS Release 12.2(33)SRD is not supported.

  Workaround: Remove the **no service image-version efsu** configuration by the default **service image-version efsu** and continue the upgrade process.

  Further Problem Description: If any of the following Config, Exec or ROMMON variables are set, the SSO-based ISSU will not be blocked:

  Config:

  "no service image-version efsu",

  "no service image-version compatibility",

  Exec:

  "issu image-version compatibility disable",

  ROMMON variable:

  RED_MODE = "RPR_PLUS’

  RED_MODE_SSO

  RF_REDUN_COMP = 1

  When performing any ISSU upgrade from SRB/SRC to SRD, make sure none of the above overrides is set on the router. The **service image-version efsu** command detects the incompatibility and puts the router in RPR mode.

- CSCsv92088

  Symptoms: BACKPLANE_BUS_ASIC-4-DEV_RESET error interrupts generated by SIP-400 module, causing traffic interruption.

  Conditions: Occurs when PPPoE traffic ingresses a SIP-400 line card on a Cisco 7600 Series router running Cisco IOS Release 12.2SR.

  Workaround: There is no workaround.

- CSCsv97273

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

Signal = 11 Vector = 0x1400

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

Workaround: There is no workaround.

- CSCsv99716

  Symptoms: A Cisco 10000 series router may crash at issu_print_memory while doing a loadversion.

  Conditions: The symptom is observed on a Cisco platform, when enabling the debug command **debug issu all** in the router and doing a loadversion.

  Workaround: Do not turn on ISSU debug.

- CSCsw14845

  Symptoms: An access-list with multiple ports in a single entry only programs the first port into TCAM. All subsequent ports are are not processed according to the access-list entry.

  For example, the following access-list should block both SSH (TCP port 22) and Telnet (TCP port 23), but Telnet is permitted.

  ip access-list extended deny_ssh_and_telnet deny tcp any any eq 22 telnet permit ip any any

  Conditions: Occurs when there is an extended named access-list with multiple ports in a single access-list entry. This only applies to transit traffic since traffic destined to the router is process-switched and processed in software.

  Workaround: There is no workaround.

- CSCsw16698

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

  Other Symptoms:

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

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

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

  1.3 Output of "show run" is delayed.

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

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

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

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

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

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

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

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

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

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

- CSCsw25255

  Symptoms: A Catalyst 6500 or Cisco 7600 router may not send back a BPDU with agreement flag in response to a proposal on its root port, causing slow convergence on the designated bridge.

  Conditions: This is seen on Catalyst 6500 switches running any version of Cisco IOS Release 12.2(33)SXH. This is seen on Cisco 7600 routers running any version of Cisco IOS Release 12.2SR.

  Workaround: The problem does not occur if **debug spanning-tree event** is enabled. This can be a suitable workaround in an environment with a small number of VLANs if the debug does not impact CPU usage.

- CSCsw31019

  Symptoms: A Cisco router crashes.

  Conditions: This symptom is observed if the **frame-relay be 1** command is issued under "map-class frame-relay <name>" configuration.

  Workaround: There is no workaround.

- CSCsw37053

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

  Conditions: Occurs under the following scenario:

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

  2. The recirculation VLAN has the wrong VPN number.

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

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

- CSCsw41041

  Symptoms: Cisco ASR1000 routers running Cisco IOS software are vulnerable to a crash when PPTP packets are sent to the router.

  Conditions: Occurs under normal operating conditions.

  Workaround: CoPP may be configured on the device to protect the management and control planes and to workaround this risk by explicitly permitting only authorized traffic sent to the route processor in accordance with existing security policies and configurations. The following example can be adapted to your network.

  !-- Permit all TCP and UDP PPTP 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 100 permit tcp any any eq 1723 access-list 100 permit udp any any eq 1723

  !-- 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-pptp-class match access-group 100

  !-- Create a Policy-Map that will be applied to the !-- Control-Plane of the device

policy-map drop-pptp-traffic class drop-pptp-class police 8000 conform-action drop

!-- Apply the Policy-Map to the Control-Plane of the !-- device

control-plane service-policy input drop-pptp-traffic

- CSCsw43499

  Symptoms: Accounting start sent on DHCP OFFER rather than ACK.

  Conditions: This issue can cause accounting irregularities if the DHCP process does not complete. For example, with active-active Cisco Intelligent Services Gateway (ISG) redundancy, two DHCP OFFERs will be sent, but only one will be accepted. Since accounting records are generated for both OFFERs, they will be duplicates of each other.

  Workaround: There is no workaround.

- CSCsw47475

  Symptoms: Cisco 7600 router has multiple E1s that randomly flap.

  Conditions: Occurs on a router with RSP720, SIP-200 and 8xCHT1/E1 SPA installed.

  Workaround: There is no workaround.

- CSCsw52698

  Symptoms: The following error message is displayed:

  %BACKPLANE_BUS_ASIC-4-DEV_RESET: Backplane Bus Asic reset, interrupt [0x062D]=0x0008

  Conditions: Symptom reported by 7600-SIP-400 cards on 7600 Series Routers when PPPoE connections are terminated via the 7600-SIP-400 cards.

  Workaround: There is no workaround.

- CSCsw70125

  Symptoms: A Cisco 7600 SIP-400 with POS interfaces encapsulated with IETF frame-relay may incorrectly set 0x800 as Network Layer Protocol Identifier (NLPID) for hardware assisted multicast IP packets. The correct value is 0xCC.

  Conditions:

  A. IP unicast packets in hardware path do not have this problem.

  B. IP multicast or unicast packets in software path do not have this problem.

  C. Problem reproducible in Cisco IOS Release 12.2(33)SRA2, 12.2(33)SRA7, and 12.2(33)SRC2.

  Workaround: There is no workaround.

- CSCsw71208

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

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

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

- CSCsw73956

  Symptoms: During health monitor failure, platform action was taken immediately but platform action should be taken from gold TCL policy.

  Conditions: Occurs when health monitor test failure crosses failure threshold.

  Workaround: There is no workaround.

- CSCsw77205

  Symptoms: ES20 line cards crashing in a loop while using a anything over MPLS (AToM) VC with Cisco Intelligent Services Gateway (ISG).

  Conditions: The issue is seen on all the ES20 cards installed in a Cisco 7609 router running Cisco IOS Release 12.2(33)SRC2.

  Workaround: Manually shutdown the AToM interfaces and ISG interfaces to stop the crashes.

- CSCsw78939

  Symptoms: No new sessions can come up using VPDN after a few days.

  Conditions: The root cause is that we leak and run out of SSM switch IDs.

  Workaround: There is no workaround.

- CSCsw82507

  Symptoms: DPM on secondary Cisco Intelligent Services Gateway (ISG) does not clear its session despite the fact that a DHCP termination message is sent. Even though the binding is cleared, the session persists until the idle timeout expires or the session is manually cleared.

  Conditions: Occurs when multiple DHCP relay agents are present between clients and DHCP server.

  Workaround: The session may expire due to idle timeout or be manually cleared.

- CSCsw89962

  Symptoms: Ping across CE routers fails.

  Conditions: Occurs when "bidir" is configured.

  Workaround: There is no workaround.

- CSCsw92379

  Symptoms: Many "IP ARP: Sticky ARP entry invalidated" syslog messages appear, and the RP reloads unexpectedly.

  Conditions: This symptom is observed when a linecard is swapped while thousands of DHCP snooping bindings are present and the **ip sticky-arp** command is configured.

  Workaround: Configure the **no ip sticky-arp** command.

- CSCsx20566

  Symptoms: Traffic through SIP400 stops or SIP400 displays minor error in **show mod** output.

  Conditions: Seen sometimes on doing RPR+ switchover in a chassis that supports hot fabric synchronization.

  Workaround: Reset the line card.

- CSCsx21231

  Symptoms: SPA-24CHT1-CE-ATM will remain out of service on a SIP-400 because of a missing API.

  Conditions: This issue will be seen during boot up on a Cisco 7600 router with SPA-24CHT1-CE-ATM and SIP-400.

  Workaround: There is no workaround.

- CSCsx22512

  Symptoms: After clearing the DHCP snooping bindings, renewing from the database and reloading the line card, snooping bindings are lost.

Conditions: Occurs when DHCP snooping is configured to store bindings in the database on the flash disk.

Workaround: There is no workaround.

- CSCsx23566

  Symptoms: All Layer 3 traffic is silently dropped on the ES40 line card after the module is reset.

  Conditions: Occurs when Layer 2- and Layer 3-based Ethernet Virtual Circuits are configured on the ES40. This happens after an RSP fail over or when the module is reset using the **hw-module module # reset** command.

  Workaround: Reload the router.

- CSCsx27659

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

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

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

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

- CSCsx37313

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

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

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

Open Caveats—Cisco IOS Release 12.2(33)SRD

This section describes possibly unexpected behavior by Cisco IOS Release 12.2(33)SRD. All the caveats listed in this section are open in Cisco IOS Release 12.2(33)SRC. This section describes only severity 1, severity 2, and select severity 3 caveats.

- CSCsk23247

  Symptoms: In MPLS/VPN network, some prefixes received on the provider edge (PE) via eBGP are installed into the VPN routing/forwarding (VRF) Border Gateway Protocol (BGP) table, but not into the VRF routing table. As a result, the prefix will not be advertised to the other BGP peers and the route reflector.

  Conditions: This problem is seen on PE running Cisco IOS Release 12.2(27)SBB5 and Cisco IOS Release 12.2(31)SB1b.

  Workaround: Advertise smaller prefixes. For example, if the failing prefix is a /25, the workaround is to advertise two times a /26 prefix.

- CSCsk35801

  Symptoms: Bulk-sync failure message is printed in console.

  Conditions: This happens during stateful switchover (SSO).

  Workaround: There is no workaround.

- CSCsk94853

  Symptoms: Bridge domain configuration not synchronized with standby router.

  Conditions: Occurred on a Cisco 7600 router running Cisco IOS Release 12.2(33)SRC.

  Workaround: Create the range first, exit the range, then apply the bridge-domain again.

- CSCsl77577

  Symptoms: Convergence time degraded 50%.

  Conditions: This is seen when a low-cost link is shut and traffic is diverted to use the high-cost link. The MPLS forwarding plane gets programmed with the new outgoing label.

  Workaround: There is no workaround.

- CSCsm97014

  Symptoms: MLPoFR with the member group interface as crackerjack PA (PA-MC-2T3-EC) is configured. On applying a simple policy along with RTP header compression virtual template, the connectivity breaks.

  Conditions: This is seen across PA (PA-MC-2T3-EC) and on applying both header compression and QoS policy.

  Workaround: There is no workaround.

- CSCso07705

  Symptoms: Tracebacks seen on Cisco 7200 router.

  Conditions: Occurs when SSH is used to connect to Distributed Link Fragmentation and Interleaving over Leased Lines (dLFIoLL) multilink IP address.

  Workaround: There is no workaround.

- CSCso42210

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

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

  Workaround: There is no workaround.

- CSCso56733

  Symptoms: Error messages and tracebacks in pm_get_standby_vlan.

  Conditions: Occurs after adding more traffic engineering (TE) tunnels over port-channel interface beyond the 1000 previously configured.

  Workaround: There is no workaround.

- CSCsq37953

  Symptoms: Junk value is seen in stand-by router.

  Conditions: Junk value is observed in stand-by router when normal ATM PVC is created. After switch-over, junk value is seen in both active and stand-by routers.

  Workaround: There is no workaround.

- CSCsr01404

  Symptoms: Multicast traffic is blocked due to duplicated **interface tunnel** configuration after Hot Standby Routing Protocol (HSRP) failover.

Conditions: Occurred during testing of an internal build of Cisco IOS Release 12.2SR. All of the affected tunnels are configured with tunnel protection.

Workaround: Remove the configuration from all the tunnels where double configuration is seen in the running configuration. Reapply the proper configuration and the router will start forwarding the multicast traffic.

- CSCsr57780

  Symptoms: Drop rate and offer rate counters are incorrect with Distributed Link Fragmentation and Interleaving over Frame Relay (dLFIoFR).

  Conditions: Occurs when Cisco 7600 router is configured for shaping of frame-relay traffic.

  Workaround: There is no workaround.

- CSCsr86826

  Symptoms: A standby SP may experience a memory leak in the mls-hal-agent process.

  Conditions: This has been experienced on a Cisco 7600 router with dual SUP720s running either Cisco IOS Release 12.2(33)SRC or Cisco IOS Release 12.2(33) SRC1. The router is configured for multicast.

  Workaround: There is no workaround.

- CSCsu27304

  Symptoms: IP Control Protocol (IPCP) goes down during initial negotiation, then gets re-negotiated.

  Conditions: Occurred while bringing up the PPPoEoE session. Occurred on a Cisco 7600 router.

  Workaround: There is no workaround.

- CSCsu35597

  Symptoms: Renaming a directory gives error message.

  Conditions: This happens on a Cisco router running Cisco IOS Release 12.4(20)T1.fc2 image

  Workaround: There is no workaround.

- CSCsu38597

  Symptoms: VPN routing/forwarding (VRF) ping from PE to locally attached CE fails.

  Conditions: Problem is seen with WAN interfaces.

  Workaround: Reconfigure the controller.

- CSCsu40667

  Symptoms: A Cisco 7600 series router may fail to install some NetFlow entries even if NetFlow table utilization is low.

  Conditions: Occurs while flows are ingressing on ES20 module.

  Workaround: There is no workaround.

  Further Problem Description: The **show mls netflow table-contention detail** command will show a heavy ICAM table utilization, while TCAM utilization is small.

```
Router#sh mls net table-contention det
Earl in Module 1
Detailed Netflow CAM (TCAM and ICAM) Utilization
================================================
TCAM Utilization : 0%
ICAM Utilization : 98%
Netflow TCAM count : 152
Netflow ICAM count : 126
```

```
Netflow Creation Failures : 388663
Netflow CAM aliases : 0
```

- CSCsu49189

  Symptoms: Frame-Relay fragment output not seen when modifying the attached map-class.

  Conditions: Occurs on a Cisco 7200 router.

  Workaround: Detach and attach Frame-Relay fragment.

- CSCsu56519

  Symptoms: V-access counters not updated with Distributed Link Fragmentation and Interleaving over ATM (DLFIoATM) in SIP-200 and SIP-400.

  Conditions: Occurs When DLFIoATM is configured and the **show interface virtual-access <>** is issued on the RP console.

  Workaround: There is no workaround.

- CSCsu64379

  Symptoms: The following error is displayed:

  ```
  %SW_MGR-SP-STDBY-3-CM_ERROR_CLASS: Connection Manager Error: Class ADJ: - bind all.
  ```

  Conditions: Occurs when anything over MPLS (AToM) VC is configured on VLAN and travels over a port-channel interface.

  Workaround: Configure VC to take a path that avoids the port-channel interface.

- CSCsu69590

  Symptoms: After Flex Link failover, connectivity may be lost. Configured VLANs might be pruned on active link, causing VLAN interface to go down.

  Conditions: This usually happens after the second Flex Link failover.

  Workaround: Remove the Flex Link configuration from the interface, then reconfigure it.

- CSCsu79340

  Symptoms: Cisco router crashed while Intermediate System-to-Intermediate System (IS-IS) is coming up.

  Conditions: Occurred on a Cisco router running Cisco IOS Release 12.2(33)SRC2.

  Workaround: There is no workaround.

- CSCsu87248

  Symptoms: Router crashes while adding flexible NetFlow.

  Conditions: Occurred on a router running Cisco IOS Release 12.2(33)SRC1.

  Workaround: There is no workaround.

- CSCsu87288

  Symptoms: Router displays the following error message:

  ```
  Sep 15 03:35:17.023 UTC: %SYS-SP-3-CPUHOG: Task is running for (4000)msecs, more than
  (2000)msecs (2/0),process = NDE - IPV4. -Traceback= 91BBFE0 91B7DA0 91B851C 91B887C
  91B8A20 91BBC20 91A8398 91E14E0 8A19ADC 8A19E4C 8A19EB4 8403614 84006C4 83FE6AC
  83FD854 83FD7FC Sep 15 03:35:19.027 UTC: %SYS-SP-3-CPUHOG: Task is running for
  (2000)msecs, more than (2000)msecs (4/2),process = NDE - IPV4. -Traceback= 91BBFE0
  91B7DA0 91B851C 91B887C 91B8A20 91BBC20 91A8398 91E14E0 8A19ADC 8A19E4C 8A19EB4
  8403614 84006C4 83FE6AC 83FD854 83FD7FC Sep 15 03:35:21.031 UTC: %SYS-SP-3-CPUHOG:
  Task is running for (4000)msecs, more than (2000)msecs (5/2),process = NDE - IPV4.
  -Traceback= 91A7DF8 91BC19C 91B7F6C 91B851C 91B887C 91B8A20 91BBC20 91A8398 91E14E0
  8A19ADC 8A19E4C 8A19EB4 8403614 84006C4 83FE6AC 83FD854
  ```

Conditions: Occurred when NetFlow was enabled.

Workaround: There is no workaround.

- CSCsu96730

  Symptoms: Intelligent Services Gateway (ISG) traffic from one user to another may fail if the packet needs to be processed by the RP in a Cisco 7600.

  Conditions: Occurs when ISG is configured and packets are switched from one subscriber to a second subscriber on another interface.

  Workaround: There is no workaround.

- CSCsu96744

  Symptoms: Multicast packets are not being forwarded.

  Conditions: Symptom observed on Cisco 7600 series routers configured with egress multicast replication mode.

  Workaround: If performance impact is acceptable, configure ingress multicast replication mode.

- CSCsu97177

  Symptoms: Switch may crash while querying IPv6 MIB.

  Conditions: This crash was seen while querying cInetCidrRouteEntry (1.3.6.1.4.1.9.10.85.7.1).

  Workaround: Exclude the MIB from queries.

- CSCsu99573

  Symptoms: Cisco router crashes when Open Shortest Path First (OSPF) neighbor is being configured in non-base topology and IP address of the neighbor does not fall into range of any existing interface.

  Conditions: This crash will only occur when OSPF is configured to support multi-topology routing, and neighbor statements are used in the submode for a non-base topology.

  Workaround: Configure the neighbor with this IP address in the base topology first.

- CSCsv04381

  Symptoms: Pseudowire redundancy is not working as expected when the backup peer configuration is performed on a Cisco 7600 router.

  Conditions: Occurs when the Cisco 7600 is one of the two ends of the primary pseudowire.

  Workaround: There is no workaround.

- CSCdy26008

  Symptoms: The negotiated IP address is not cleared from an asynchronous interface when a call ends, even though the IP address is returned properly to the IP peer pool.

  Conditions: This symptom is observed when the peer is configured to dial in to the network access server (NAS) and to obtain an IP address through IP Control Protocol (IPCP) negotiations with the NAS. The NAS is configured with pools of IP addresses to be allocated to the peer when the peers generate a PPP call to the NAS. The NAS is also configured to authenticate the peer through RADIUS.

  Workaround: There is no workaround.

- CSCee63182

  Symptoms: A Cisco router may crash or may stop responding.

Conditions: This has been always seen with an atm interface only when a rate-limit command is enabled on the interface. The crash occurs when an interface that is configured with a **rate-limit** command is deleted by entering the **no interface** command and then reenabled by entering the **interface** command.

Workaround: Remove the rate-limit configuration from the interface before deleting the interface.

Further Problem Description: Happens under very specific circumstances and the crash is seen randomly.

- 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**.

- CSCek48205

  Symptoms: The output counters for a Multilink Frame Relay (MFR) bundle interface may not be updated correctly.

  Conditions: Occurs after the same interface is deleted and recreated.

  Workaround: There is no workaround.

- CSCin91677

  Symptoms: The Unavailable Seconds (UAS) that are displayed in the output of the **show controllers serial** *slot/port* command are incorrect. The display of the UAS starts only after 20 contiguous severely errored seconds (SES) instead of after 10 contiguous SES.

  Conditions: This symptom is observed on a Cisco 7200 series that is configured with a PA-T3+ port adapter.

  Workaround: There is no workaround.

- CSCsb98906

  Symptoms: A memory leak may occur in the "BGP Router" process.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.0(26)S6, that is configured for BGP, and that has the **bgp regexp deterministic** command enabled.

  Workaround: Disable the **bgp regexp deterministic** command.

- CSCse26506

  Symptoms: When you perform an OIR of an ATM line card, a CPUHOG condition may occur in the "BGP Event" process.

  Conditions: This symptom is observed when the ATM line card is configured with about 15,000 /32 routes.

  Workaround: There is no workaround.

  Further Problem Description: The ATM line card connects to about 15,000 different gateways, each of which is covered by its own /32 route. In addition, there is a less specific route that covers everything. The symptom occurs when BGP attempts to remove a large number of these tracked entries without suspending any.

- CSCsf25157

Symptoms: An IPv6 ping may fail when the **atm route-bridged ipv6** command is enabled.

Conditions: This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.3(22.13), interim Release 12.4(13.9), or Release 12.4(13b) and that is configured for QoS.

Workaround: There is no workaround.

- CSCsg11616

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

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

  Workaround: There is no workaround.

- CSCsh48947

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

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

  Workaround: There is no workaround.

- CSCsi88974

  Symptoms: While configuring a mediation device (MD), if the MediationSrcInterface is set to loopback interface, traffic will cause MALLOC failures.

  Conditions: Problem is seen when traffic rate is equal to or greater than 8000 packets per second.

  Workaround: Do not use loopback0 as MD source interface.

- CSCsj34557

  Symptoms: Router displays following error message and reloads:

  ```
  Jun 18 06:12:23.008: event flooding: code 10 arg0 0 arg1 0 arg2 0
  %SYS-3-OVERRUN: Block overrun at E5D8310 (red zone 00000000) -Traceback= 0x6080CEB0
  0x60982108 0x60982EC0 0x6098511C 0x609853BC %SYS-6-MTRACE: mallocfree: addr, pc
  662B5B1C,608A6F3C 0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6 662B5B1C,608A6F3C
  0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6 %SYS-6-MTRACE: mallocfree: addr, pc
  662B5B1C,608A6F3C 0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6 662B5B1C,608A6F3C
  0,608A6D9C 662B5B1C,608A6D4C 662B5B1C,300001A6 %SYS-6-BLKINFO: Corrupted redzone blk
  E5D8310, words 6088, alloc 61FE2638, InUse, dealloc 80000000, rfcnt 1 -Traceback=
  0x6080CEB0 0x609681D4 0x6098211C 0x60982EC0 0x6098511C 0x609853BC %SYS-6-MEMDUMP:
  0xE5D8310: 0xAB1234CD 0xFFFE0000 0x0 0x63894208 %SYS-6-MEMDUMP: 0xE5D8320: 0x61FE2638
  0xE5DB2D0 0xE5D8144 0x800017C8 %SYS-6-MEMDUMP: 0xE5D8330: 0x1 0x0 0x1 0x64B53478
  ```
  %Software-forced reload

  Conditions: Occurred on a Cisco 7200 running the c7200-ik9s-mz.124-7a.bin image.

  Workaround: There is no workaround.

- CSCsj46607

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

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

  Workaround: There is no workaround.

- CSCsj78403

Symptoms: A router may crash when the **clear ip bgp** command is entered.

Conditions: Occurs on devices running BGP and configured as a route reflector client with conditional route injection configured.

Workaround: Unconfigure conditional route injection.

- CSCsk28748

  Symptom: When an IMA group subinterface (atm1/ima1.14016) is configured before a **no shut**is done on the IMA group interface, the maximum value VBR-NRT peak cell rate (PCR) option is displayed as 1536/1920(T1/E1) instead of 1523/1904.

  Conditions: Occurred when IMA group subinterface is configured before assigning ATM interface to the IMA group.

  Workaround: Configure the IMA group interface first and then configure image group sub- interface.

- CSCsk48366

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

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

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

  Workaround: There is no workaround.

- CSCsl00472

  Symptoms: A Cisco router unexpectedly reloads with memory corruption after showing multiple "%SYS-2-INPUT_GETBUF: Bad getbuffer" messages

  Conditions: Occurs during normal operation.

  Workaround: There is no workaround.

- CSCsm28287

  Symptoms: After shutting down a GRE tunnel interface, the active RP crashed and switchover took place. The following error message was displayed:

  ```
  %ALIGN-1-FATAL: Illegal access to a low address 13:02:45 UTC Fri Jan 18 2008 addr=0xD,
  pc=0x7144A5A0, ra=0x7209FFF8, sp=0x5ABEE90 SLOT0:01:40:03: %DUMPER-3-PROCINFO: pid =
  16409: (sbin/ios-base), terminated due to signal SIGBUS, Bus error (Invalid address
  alignment) SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: zero at v0 v1
  SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: R0 00000000 7A5FD854 EF4321F9
  7A6452D0 SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: a0 a1 a2 a3 SLOT0:01:40:03:
  %DUMPER-3-REGISTERS_INFO: 16409: R4 EF4321CD 0000000B 0000000B 00000000
  SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: t0 t1 t2 t3 SLOT0:01:40:03:
  %DUMPER-3-REGISTERS_INFO: 16409: R8 7CB96E10 00FDDBE0 00000000 EFFFFFFF
  SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: t4 t5 t6 t7 SLOT0:01:40:03:
  %DUMPER-3-REGISTERS_INFO: 16409: R12 00000000 F7E8E12F 00000000 00000000
  SLOT0:01:40:03: %DUMPER-3-REGISTERS_INFO: 16409: s0
  ```

  Conditions: Occurred on a Cisco 7200 running an internal build of Cisco IOS Release 12.2SX.

  Workaround: There is no workaround.

- CSCsm55817

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

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

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

- CSCso67602

  Symptoms: When PVC is configured under ubr 5000, the router crashes.

  Conditions: Occurred on a Cisco 7200 router running an internal build of Cisco IOS Release 12.2SB.

  Workaround: There is no workaround.

- CSCsq49176

  Symptoms: Router bus error crash on invalid address:

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

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

  Workaround: There is no workaround.

- CSCsq51378

  Symptoms: ATM PA Interface with no cables connected shows up/up after forced redundancy.

  Conditions: Occurred under the following scenario:

  - No cables attached to Fast Ethernet or ATM interface.
  - Issue **no shut** on interface.
  - The **show ip int brief** command shows interface status up/protocol down.
  - After **redundancy force** command is entered, interface shows up/up (no cables connected).

  This affects Fast Ethernet interfaces and ATM interfaces on WS-x6582-2PA/PA-2FE-TX and PA-A3-OC3-MM. It does not affect Supervisor ports or Serial Interfaces.

  Workaround: There is no workaround.

- CSCsq53542

  Symptoms: After stateful switchover (SSO) there may be loss of multicast packet delivery for 10 or more seconds.

  Conditions: Occurs when multicast routing is enabled in the default mode.

  Workaround: If there are no mStatic or mBGP routes, the following configuration will avoid the problem:

  ```
  Router(config)#ip multicast rpf multitopology
  Router(config)#global-address-family ipv4 multicast
  Router(config-af)#topology base
  Router(config-af-topology)#use unicast base
  Router(config-af-topology)#
  ```

- CSCsq80495

  Symptoms: If a service instance is already configured with encapsulation untagged and if a user tries to configure another service instance with encapsulation untagged, then this service instance configuration is lost.

  Conditions: This issue happens only if there is encapsulation untagged already configured on another service instance.

  Workaround: Remove the encapsulation untagged for other service instance.

- CSCsq84624

  Symptoms: A Cisco router might crash when **debug condition portbundle ip 10.1.1.1 bundle 0** is configured.

Conditions: Occurs when this command is executed prior to configuring **ip portbundle**.

Workaround: There is no workaround.

- CSCsr09062

  Symptoms: Cisco 7200 crashes due to memory corruption.

  Conditions: Occurs when MLP+QoS is configured on a Cisco 7200 router. QoS policy is having bandwidth, change the BW parameter and flap the multilink using **clear int multilink1** to see the crash.

  Workaround: There is no workaround.

- CSCsr24171

  Symptoms: "snmpEngineTime" is not stateful switchover (SSO) aware. The value changes after switchover.

  Conditions: Seen only in high-availability systems after switchover.

  Workaround: There is no workaround.

- CSCsr26025

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

  Conditions: Occurs under the following scenario:

  - Border Gateway Protocol (BGP) with two neighbors sending a default gateway.
  - Static route "0.0.0.0/8 to null 0" is configured.
  - Failover takes place and RIB is not updated.

  Workaround: There is no workaround.

- CSCsr26663

  Symptoms: Some Gateway Load Balancing Protocol (GLBP) forwarders may flap to a GLBP group peer. This will cause a momentary drop in network traffic for clients associated with the flapping forwarders.

  Conditions: The problem only occurs when GLBP is using low or default timer values on a router that has a large number of GLBP groups configured.

  Workaround: Larger GLBP timer values may be used in order to prevent forwarders flapping, however these larger timer values will increase the delay in network recovery when a GLBP router completely fails.

- CSCsr27980

  Symptoms: When adding a class into existing policy-map and the total bandwidth exceeds system defined limits, it gets accepted in MQC. On removing another class from the same policy map, tracebacks are thrown, and the system is hogged completely.

  Conditions: This symptom is seen when the total bandwidth for the classes exceeds the platform defined limits.

  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.

- CSCsr44492

  Symptoms: Certain QoS configurations are such that the hierarchical queuing framework (HQF) layer is collapsed and then later modification to those configuration causes the HQF layer to un-collapse. This may put the router into an unpredictable state or cause some QoS parameter values to be wrong.

  Conditions: Occurs under the following scenario:

  1. Configure a policy as follows:

  ```
  policy-map p1 class class-default sh av <>
  ```
  2. Attatch the poliy to logical target.

  3. Modify the policy as follows:

  ```
  policy-map p1 class prec1 bandwidth <>
  ```
  This causes the HQF layer to un-collapse, which the router will not handle properly.

  Workaround: Reload the router.

- CSCsr49701

  Symptoms: Router may reset after removing a large VPN routing/forwarding (VRF) configuration.

  Conditions: Occurred on a Cisco 10000 Series Router running Cisco IOS Release 12.2(33)XNA following the removal of a VRF with 200,000 routes.

  Workaround: The issue does not occur when a VRF of 160,000 routes was removed. Do not allow the number of routes to exceed this number.

- CSCsr55713

  Symptoms: A crash occurs.

  Conditions: The crash is caused by a ping across an ISATAP tunnel. The symptom is observed only in Cisco IOS Release 12.4(15)T7 on the Cisco 7200 (it is not known to affect other platforms), since the crash is dependent on the Cisco IOS memory map (which varies with each image).

  Workaround: There is no workaround.

- CSCsr55922

  Symptoms: The EIGRP IPv6 process may incorrectly select a router-ID from the 127.0.0.0 address range.

  Symptoms: The same router-ID may be selected on two separate Cisco routers configured for EIGRP IPv6. External prefixes advertised by one of the EIGRPv6 routers will be ignored by the receiving EIGRPv6 router due to the fact the routerID contained in the external data portion of the prefix matches the receiving routerID; a loop prevention method.

  Workaround: Manually configure a router-ID under the EIGRP IPv6 process with **router-id** *address* command.

- CSCsr62811

  Symptoms: An ASR 1000 series router may experience an unforced system reload after operating for several hours.

  Conditions: The system must be running for several hours and have QoS configured on one or more interfaces.

  Workaround: There is no workaround.

  Further Problem Description: This problem arises from a memory leak. Closely monitor the system's memory usage to ensure that it is not running low.

- CSCsr82917

  Symptoms: A traceback is observed when an ANCP session is setup.

  Conditions: This symptom occurs when setting up an ANCP session.

  Workaround: There is no workaround.

- CSCsr90248

  Symptoms: Changing any of the parameters of a route-map does not take effect.

  Conditions: Occurs when using a BGP aggregate-address with an advertise map.

  Workaround: Delete the aggregate-address statement and then put it back for the change to take effect.

- CSCsr96042

  Symptoms: ASR1000 Router crashes.

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

  Workaround: There is no workaround.

- CSCsr96468

  Symptoms: The following may be seen on a Catalyst 3750 if an HSRP version 2 group is configured after an HSRP version 1 group:

  ```
  Vlan5 - Group 300 (version 2) State is Init (virtual MAC reservation failed)
  ```

  The correct behavior is for the HSRP version 2 group to be rejected since the Catalyst 3750 only supports MAC addresses for one HSRP version at any one time.

  Conditions: This only affects the Catalyst 3750 platform.

  Workaround: Remove the HSRP version 2 group.

- 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.

- CSCsu31444

  Symptoms: A BR continuously displays errors messages on the console.

  ```
  Router#%Error: timeout value is less than threshold 5000 %Error: timeout value is less
  than threshold 5000 %Error: timeout value is less than threshold 5000 %Error: timeout
  value is less than threshold 5000 %Error: timeout value is less than threshold 5000
  %Error: timeout value is less than threshold 5000 %Error: timeout value is less than
  threshold 5000 %Error: timeout value is less than threshold 5000 %Error: timeout value
  is less than threshold 5000
  ```

  OER jitter probes are not created because of this error.

  Conditions: This symptom is observed with the jitter probe configuration below for VOIP optimization:

oer-map BRANCH 20 match traffic-class access-list Optimize_Voice_Traffic set mode route control set mode monitor fast set resolve mos priority 1 variance 30 set resolve delay priority 2 variance 30 set active-probe jitter 10.100.10.1 target-port 1025 codec g729a << set probe frequency 4

Workaround: The workaround is to set higher probe frequency (higher than 5)

- CSCsu32104

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

  Conditions: Unknown at this time.

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

- CSCsu36836

  Symptoms: TCL scripts and policies attempting to work with open files and sockets simultaneously may not operate properly. One symptom is the **vwait** command may fail by reporting "would wait forever".

  Conditions: Occurs when a TCL script opens both a file and a client or server socket simultaneously.

  Workaround: Open and close files and sockets separately. Avoid having them open simultaneously.

- CSCsu46871

  Symptoms: Unable to attach service policy to VT when bandwidth is configured in class default.

  Conditions: Occurs when DLFI over ATM is configured while trying to attach service policy to VT when bandwidth is configured in class default.

  Workaround: Configure bandwidth in user defined class and attach to VT.

- CSCsu55145

  Symptoms: Router crashes due to critical software exception.

  Conditions: Occurs on a Cisco ASR 1000 running Cisco IOS Release 12.2.

  Workaround: There is no workaround.

- CSCsu62667

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

  Conditions: Occurs following a SSO switchover.

  Workaround: There is no workaround.

- CSCsu64323

  Symptoms: The **show vpdn history failure** command should show the history of session failures due to entering incorrect password, but it does not show any history.

  ```
  Router#show vp hi fa % VPDN user failure table is empty
  ```
  Conditions: The problem was seen with Cisco 7201 running Cisco IOS Release 12.2(33)SRC1. No problem with Cisco IOS Release 12.4(4)XD9.

  Workaround: There is no workaround.

- CSCsu67637

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

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

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

- CSCsu73128

  Symptoms: Router crashes.

  Conditions: Occurs when large number of remote end points try to connect to the gateway at the same time. The router may crash if "rsa-sig" is used as authentication method.

  Workaround: There is no workaround.

- CSCsu87181

  Symptoms: When a Cisco 7600 router is running Cisco IOS Release 12.2(33)SRD and EVC MAC security is enabled on a service instance, after the encapsulation is changed on the service instance, the MAC address can not be learned dynamically for that service instance.

  Conditions: This problem only occurs when the encapsulation is changed on a service instance.

  Workaround: After the encapsulation is changed, remove the **mac security** command, then re-configure the command.

- CSCsu88256

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

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

  Workaround: There is no workaround.

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

- CSCsu89550

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

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

  Workaround: Remove the control-plane policy.

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

- CSCsu97934

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

  Conditions: Unknown.

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

Resolved Caveats—Cisco IOS Release 12.2(33)SRD

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(33)SRD. This section describes only severity 1, severity 2, and select severity 3 caveats.

Miscellaneous

- CSCdv07156

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

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

  Workaround: There is no workaround.

- CSCeb69473

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

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

```
router>connect 192.168.0.1 login /terminal-type aaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Trying 192.168.0.1...Open login:
*** System received a SegV exception *** signal= 0xb, code= 0x1100, context=
0x82f9e688 PC = 0x61616160, Vector = 0x1100, SP = 0x833ae5a8
```

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

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

  Configuring Authorization
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hsec_c/part05/schathor.htm

  ACS 4.1 Command Authorization Sets
  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/ user/SPC.html#wpxref9538

  ACS 4.1 Configuring a Shell Command Authorization Set for a User Group
  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/ user/GrpMgt.html#wp480029

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

  Role-Based CLI Access

  http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_role_base_cli.html

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

Infrastructure Protection on Cisco IOS Software-Based Platforms Appendix B-Controlling Device Access
http://www.cisco.com/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

- 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.

- CSCec51750

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

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

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

- CSCec72958

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

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

  Workaround: There is no workaround.

- CSCee19691

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

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

  Workaround: There is no workaround.

- CSCee30355

  Symptoms: A Cisco router may experience a memory leak. The "Holding" column in the output of the **show process memory** command shows that the "VTEMPLATE Backgr" process allocates memory without freeing it. This column will continue to grow until all the memory is consumed.

  Conditions: This symptom is observed on a Cisco router that is configured for RIP version 2. In addition configuration with 800+ virtual-access interfaces using VPDN reported a memory leak for the RIP multicast group.

  Workaround: Schedule the router for a periodic reload before it completely exhausts all available memory.

- 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.

- CSCef52919

  Symptoms: A privilege level 1 user is able to log in with a higher privilege level.

  Conditions: This symptom is observed on a Cisco platform when the **aaa new-model** command is enabled, when the **privilege level** *level* command is present under the vty lines, and when the *level* argument has any value from 2 through 15.

  Workaround: Do not configure privilege level 1 but configure any other privilege level.

- CSCeg80842

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

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

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

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

- CSCeg86665

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

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

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

- CSCek55665

  Symptoms: When a router dials out to a client router in a particular configuration, two VPDN tunnels should be established, but only one is established.

  Conditions: This symptom is observed in an L2TP Large-Scale Dial-Out configuration when two LACs, that are connected via SGBP, are located between the router that dials out and the client. VPDN tunnels should be established between the router that dials out and each LAC, but only one VPDN tunnel is established.

  Workaround: 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.

- CSCek64889

  Symptoms: Current family of channelized SPAs will not recognize compressed MLP header and will send such packets arriving on line to host for processing.

  Conditions: Occurs when the remote end is Nortel equipment, which use the compressed MLP header format

  Workaround: There is no workaround.

- 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.

- CSCek78031

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

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

  Workaround: There is no workaround.

- CSCek78050

  Symptom: Router console hangs.

  Conditions: **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.

- CSCsb15582

  Symptoms: A PVC is unexpectedly removed from an IMA interface when one or more IMA links go down. This results in packet loss.

  Conditions: This symptom is observed on a Cisco router that has an ATM IMA interface that is configured with ATM dynamic bandwidth and no ATM oversubscription when you shut down one of the IMA links, causing dynamic bandwidth allocation to occur on the PVCs.

  Workaround: Reconfigure the PVCs with a bandwidth that can be supplied by the remaining IMA links.

- 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.

- CSCsc75381

  Symptoms: Native VLAN mismatch may not be detected when native VLAN is not consistent on two ends of 802.1Q trunk and native VLAN is not allowed on one end only. This is a case of misconfiguration, but it may result in a forwarding loop.

  For example:

  switch1(native=3)---802.1Q_trunk---(native=2)switch2

  allowed vlans on switch1: 3,4 allowed vlans on switch2: 3,4

  If STP designated port is on the switch1 side, this misconfiguration may not be detected.

  Conditions: This symptom occurs when misconfiguration is not detected.

  Workaround: Correct misconfiguration. Make native VLAN consistent on both sides or at least allow VLAN 2 (native) on trunk on switch2.

- 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.

- CSCsc87117

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

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

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

- CSCsc94969

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

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

  Workaround: There is no workaround.

- CSCsd04608

  Symptoms: When removing policy from interface, the router crashes.

  Conditions: Occurs when policy is hierarchical with child and grandchild policy.

  Workaround: There is no workaround.

- CSCsd61498

  Symptoms: The BGP bulk-synchronizes even in RPR+ mode. When the standby RP is reset, the BGP bulk-synchronization process ignores the notification and continues to bulk-synchronize.

  Condition: The symptoms are observed when the standby RP is reset or when the router is in RPR+ mode.

  Workaround: There is no workaround.

- CSCsd80349

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

  Conditions: Occur under the following scenario:

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

  Workaround: There is no workaround.

- CSCsd82457

  Symptoms: The EapOverUDP protocol cannot detect Cisco IP conference stations and wireless phones, resulting in the policy configured locally on the box for IP phones not being applied.

  Conditions: This symptom is observed with a normal EapOverUDP configuration that is used for applying the NAC policies for IP phones.

  Workaround: There is no workaround.

- CSCsd93294

  Symptoms: On a CSC-PE router with dual RPs, the following is seen on the standby RP:

  1. A near endless amount (about 45-50) of the following error messages:

```
00:34:51: %FRR_OCE-STDBY-3-GENERAL: Primary interface number and OCE do not match.
00:34:51: %SYS-STDBY-2-CHUNKFREE: Attempted to free nonchunk memory, chunk 531555D8,
data 531554E0.
```

2. Followed immediately by a crash

Conditions: This symptom occurs when performing an SSO switchover.

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.

- CSCse52929

  Symptoms: PA-MC-8TE1+ is not recognized by router.

  Conditions: PA-Mc-8TE1+ inserted on a Cisco 7200 with NPE-g2 and running ipbase, ipbasek9, entbase, or advsecurityk9 images.

  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.

- CSCsf21629

  Symptoms: In a system with a redundant Supervisor 720 Engine, the etherchannel member ports may flap after SSO.

  Conditions: The symptoms are observed when running LACP and on the first SSO only.

  Workaround: There is no workaround.

- CSCsg00173

  Symptoms: Traffic blackholing is seen in DFC-based PVLAN configuration.

  Condition: The RPF Vlan has to be programmed as secondary VLAN in the hardware tables for PVLAN to work with multicast. This condition is not satisfied in case of DFC as the primary Vlan gets programmed as RPF Vlan. The problem is not seen on the supervisor.

  Workaround: There is no workaround.

- CSCsg21394

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

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

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

- CSCsg27783

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

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

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

- CSCsg39754

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

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

  Workaround: There is no workaround.

- CSCsg40885

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

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

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

- 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.

- CSCsg72678

  Symptoms: TCAM entries are not displayed for the interface when using the **show tcam interface acl** command.

Conditions: The symptom is observed after online insertion and removal (OIR) of the DFC module in the switch.

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.

- CSCsg87559

  Symptoms: A client that has IPv6 for DHCP implemented may not receive a correct prefix.

  Conditions: This symptom is observed on a Cisco 7200 series that functions as a DHCP server, that has IPv6 for DHCP implemented, and that has the **allow-hint** DHCP IPv6 interface server configuration enabled. Note that the symptom is platform-independent.

  Workaround: There is no workaround.

- CSCsg92473

  Symptoms: The netflow shortcuts created are cleared before the full capacity of 128k flows (PFC3B) and 256k flows (PFC3BXL) is reached and before the reflexive ACL ageing timers expire. The full capacity is not achieved and active flows may start to get purged.

  Conditions: The symptoms are observed when either the traffic is from 128k or 256k different sources.

  Workaround: There is no workaround.

- CSCsg93274

  Symptoms: When a switchover occurs on the standby PRE, the router does not sent a “ciscoRFSwactNotif” notification.

  Conditions: This symptom is observed on a Cisco 10000 series when the CISCO-RF-MIB traps are enabled for host that are configured to receive traps, that is, for valid SNMP hosts that have the **snmp-server enable traps rf** command enabled.

  Workaround: Configure SNMPv2 "informs."

  Alternate Workaround: Use a static ARP configuration for the trap handlers that are configured via the **snmp-server host** command to increase the chances that the first few traps that are sent by the Cisco 10000 series are received by these trap handlers.

- CSCsg98535

  Symptoms: The **clear ipv6 pim topology** command may crash the router.

  Conditions: The symptom is observed when using the **clear ipv6 pim topology** command on the router with 30,000 (S, G) multicast (mroute) state.

  Workaround: Do not use **clear ipv6 pim topology** when the router has 30,000 mroute state. Rather, wait for three or more minutes for the mroute state to timeout and the router will remove the entry from the mroute table.

- 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#sh spanning-tree
VLAN0002 Spanning tree enabled protocol ieee Root ID Priority 32768 Address
0014.1bc4.c002 Cost 4 Port 259 (GigabitEthernet3/3) Hello Time 2 sec Max Age 20 sec
Forward Delay 15 sec
Bridge ID Priority 32768 Address 0014.1bc4.f802 Hello Time 2 sec Max Age 20 sec
Forward Delay 15 sec Aging Time 15
Interface Role Sts Cost Prio.Nbr Type ------------------- ---- --- --------- --------
--------------------------- - --- Gi3/3 Root FWD 4 128.259 P2p Gi3/4 Altn BLK 4
128.260 P2p
xs6k3#
Spanning Tree info on Standby ------------------------------ xs6k3-sdby#sh
spanning-tree
No spanning tree instance exists.
xs6k3-sdby#
```

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

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

  Impact: No spanning tree instance exists on standby.

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

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

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

- CSCsh47251

  Symptoms: A Cisco 3700 or 3800 series router crashes on bootup.

  Conditions: The crash happens only when two conditions are satisfied:

  1) An NM-xDM card is present in the box. 2) An external compact flash is present (inserted) in the box.

  Workaround: Remove the external compact flash before booting the router.

- CSCsh48919

  Symptoms: With an ATA flash card, the **dir disk0:** command will fail if any filename or directory name stored on disk0 contains embedded spaces. This applies to disk1 or disk2 as well. This situation can also occur with a compact flash (CF) card using the **dir flash:** command.

Conditions: This symptom has been observed when using a removable flash card, such as an ATA flash car or CF card, that is formatted to use DOSFS. The removable flash card is removed from the router and inserted into a laptop that is running a version of the Microsoft Windows operating system. A "New Folder" directory is created on the flash card and the flash card is removed from the laptop and re-inserted into the router. Entering the **dir** command on the router may fail to show all of the stored files or may crash the router.

Workaround: Remove or rename all files and directories having names with embedded spaces so that no file or directory names contains embedded spaces.

- CSCsh67875

  Symptoms: CLI rejects the following configuration on GSR Eng 3 GigE subinterface:

  ```
  policy-map CC_CE->PE_ETM_G=1M_M=200K
  class multicast_limit
  police cir 200000 bc 4470 be 4470 <<<<<<this is causing the error msg..
  conform-action transmit
  exceed-action drop
  ```

  Following error message was displayed:

  ```
  "Errormulti-action policy not supported on GigabitEthernet9/2.2" when trying to apply
  ingress policy CC_CE->PE_ETM_G=1M_M=200K.
  ```

  Conditions: Occurs when police command has multi-line command

  Workaround: Put command on one line, such as:

  ```
  policy-map CC_CE->PE_ETM_G=1M_M=200K
  class multicast_limit
  police cir 200000 bc 4470 be 4470 conform-action transmit exceed-action drop
  ```

- CSCsh88532

  Symptoms: Unable to change QoS trust settings on WiSM interfaces from trust CoS.

  Conditions: When certain networks need to trust DSCP or IP-precedence, WiSM could not set qos-trust values.

  Workaround: Use manual LAG configuration to set the individual gigabit interfaces and port channels to set the QoS trust to DSCP or IP-precedence instead of WiSM default CoS.

- 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.

- CSCsi17158

  Symptoms: Devices running Cisco IOS may reload with the error message "System returned to ROM by abort at PC 0x0" when processing SSHv2 sessions. A switch crashes. We have a script running that will continuously ssh-v2 into the 3560 then close the session normally. If the vty line that is being used by SSHv2 sessions to the device is cleared while the SSH session is being processed, the next time an ssh into the device is done, the device will crash.

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

Workaround: There are mitigations to this vulnerability: For Cisco IOS, the SSH server can be disabled by applying the command **crypto key zeroize rsa** while in configuration mode. The SSH server is enabled automatically upon generating an RSA key pair. Zeroing the RSA keys is the only way to completely disable the SSH server.

Access to the SSH server on Cisco IOS may also be disabled via removing SSH as a valid transport protocol. This can be done by reapplying the **transport input** command with 'ssh' removed from the list of permitted transports on VTY lines while in configuration mode. For example: **line vty 0 4 transport input telnet end**

If SSH server functionality is desired, access to the server can be restricted to specific source IP addresses or blocked entirely using Access Control Lists (ACLs) on the VTY lines as shown in the following URL:

http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swacl.html#xtocid14

More information on configuring ACLs can be found on the Cisco public website: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml

- CSCsi30873

  Symptoms: A VIP crashes when a multilink interface flaps.

  Conditions: LFI on a multilink interface and QoS is configured on a port adapter installed in the VIP. When either the multicast interface, through which traffic is flowing, is cleared or the **shut** and **no shut** commands are entered.

  Trigger: Multilink interface flap noticed.

  Impact: Impacts normal functioning of the router.

  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.

- CSCsi32894

  Symptoms: When a policy with BRR configuration has a priority class configured as well, the priority class gets a queue update with mincir set to 0 and excess ratio set to 1.

  Conditions: The issue is when a policy with BRR configuration has a priority class configured as well, the priority class gets a queue update with mincir set to 0 and excess ratio set to 1. This should not be the case for two reasons:

  a) Priority should not participate in the BRR calculations (it actually does not, but we end up invoking the queuing API with incorrect parameters).

  b) Though the platforms can determine if a queue update that they get is for a priority queue, and maybe ignore the mincir if the excess ratio is set, they do not necessarily have to do that.

Workaround: There is no workaround.

- CSCsi49008

  Symptoms: SNMP requests on VRFs may time out, and the SNMP response is sent back to a 0.0.0.0 address.

  Conditions: This symptom is observed only for SNMP requests that enter via a VRF.

  Workaround: There is no workaround.

- CSCsi54333

  Symptoms: RP inlet and outlet temperatures may display as "N/A".

  Conditions: The conditions are observed when attempting to display the environment status with the command **show environment status**. With Cisco IOS Release 12.2(18)SXF7, the RP inlet/outlet temperature sensor value displays a value of 32.

  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.

- CSCsi57927

  Symptoms: A Cisco router that is running Cisco IOS Release 12.2, Release 12.3, or Release 12.4 will show TCP connections that are hung in CLOSEWAIT state. These connections will not time out, and if enough accumulate, the router will become unresponsive and need to be reloaded.

  Conditions: This symptom occurs on a Cisco router that is running Cisco IOS Release 12.2, Release 12.3, or Release 12.4 when a **copy** *source-url* **ftp:** command is executed and the FTP server fails to initiate the FTP layer (no banner) but does set up a TCP connection. This may occur when the FTP server is misconfigured or overloaded.

  The CLI command will time out, but will not close the TCP connection or clean up associated resources. The FTP server will eventually answer and time itself out, and close the TCP connection, but the router will not clean up the TCP resources at this time.

  Workaround: Manually clear TCP resources using the **clear tcp** command, referencing the **show tcp brief** command output.

- CSCsi58211

  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 through the XenPaks.

  Workaround: The XENPAK-10GB-LW does not support >9Gbps of traffic.

- CSCsi68795

  Symptoms: A PE that is part of a confederation and that has received a VPNv4 prefix from an internal and an external confederation peer, may assign a local label to the prefix despite the fact that the prefix is not local to this PE and that the PE is not changing the BGP next-hop.

  Conditions: The symptoms are observed when receiving the prefix via two paths from confederation peers.

Workaround: There is no workaround.

Further Problem Description: Whether or not the PE will chose to allocate a local label depends on the order that the multiple paths for this VPNv4 prefix are learned. The immediate impact is that the local label allocated takes up memory in the router as the router will populate the LFIB with the labels.

- CSCsi69342

  Symptoms: Whenever Netflow is enabled on interface, all packets start getting process switched and CPU utilization goes up in IP INPUT process.

  Condition: If ip route-cache flow is enabled, it causes packets to be punted to process switching.

  Workaround: Remove Netflow commands from the configuration.

- CSCsi76842

  Symptoms: Line protocol remains down after the encapsulation on an interface is changed from FR to PPP/HDLC.

  Conditions: Occurs when you set encapsulation FR on an interface. Then change the encapsulation to PPP/HDLC.

  Workaround: Reload the sip-200 module or the SPA.

- CSCsi83287

  Symptoms: The following error occurs:

  ```
  %ALIGN-3-SPURIOUS T/B ipv6fib_gre_ipv6_classified message displayed on console
  ```
  Conditions: 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: Occurs when FRR is enabled on a TE tunnel, when 7600-SIP-600 or 7600-ES20 are used as the MPLS facing Linecard 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, swichtover 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.

- CSCsj12867

  Symptoms: The following message can be seen after executing the **write memory** command, even though the version has not been changed.

  Router# write memory

  Warning: Attempting to overwrite an NVRAM configuration previously written by a different version of the system image. Overwrite the previous NVRAM configuration?[confirm]

  The router then restarts with the following traceback:

  ```
  -Traceback= 6067F3DC 6067FB38 605E3FE8 60686384 605E3FE8 605188BC 60518830 605444D4
  60539164 6054719C 605AB65C 605AB648
  ```

  Conditions: This symptom is observed on a Cisco 7206 VXR (NPE-400) with C7200-IO-FE-MII/RJ45= or C7200-I/O=.

  Workaround: There is no workaround.

- CSCsj19019

  Symptoms: WWCP, when used in GRE mode, Netflow entries are not installed.

  Conditions: This is seen in modular Cisco IOS images.

  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.

- CSCsj56281

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

  Workaround: There is no workaround.

- CSCsj57351

  Symptoms: Router Crashes if a invalid EVC name is configured.

  Conditions: Occurs when "debug ethernet service instance error" is enabled.

  Workaround: If ether-infra debugs are enabled, then always configured a valid EVC name and attach it to service instance. Do not enable the "debug ethernet service instance error".

- CSCsj58223

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

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

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

- 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.

- CSCsj69881

  Symptoms: Router boots up very slowly.

  Conditions: Occurs with 3,000 QinQ subinterfaces with QoS applied. The QoS policy uses a class-map with a named ACL with many ACEs.

  Workaround: Avoid using large access-lists in class-map statement.

- 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.

- CSCsj87584

  Symptoms: On VSS systems, call-home inventory was sending **show idprom all** rather than **show idprom switch all**.

  Conditions: This resulted in idprom information for only one chassis being received.

  Workaround: There is no workaround.

- CSCsj87687

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

  Conditions: The symptom occurs when starting up an MPLS IOU network when all the IOU instances starting with "-e" or "-s5".

  Workaround: There is no workaround.

- CSCsj87744

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

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

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

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

Related to ATM PVC names: do not use PVC names ending with "do"

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

- 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.

- CSCsj98198

  Symptoms: The following error occurs:

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

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

  Workaround: There is no workaround.

- CSCsk03336

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

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

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsk12238

  Symptoms: Calls are torn down within a second after establishment.

  Conditions: This symptom occurs when pinging from the client to the NAS gives "Request drop link from bundle".

  Workaround: Configure the **dialer idle-timeout 0** command under the template. This will never bring down the calls nor bring down the physical link.

  template template1 dialer idle-timeout 0

- 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.

- CSCsk21328

  Symptoms: Router crashes during shutdown or deletion of interface.

  Conditions: Occurs on interfaces on which IPv6 is enabled.

  Workaround: There is no workaround.

- 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: The following two conditions are required for the issue to exist:

  - 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.

- CSCsk25838

  Symptoms: When congestion control is enabled, some CMs may get sent out of order. The actual send window size may be smaller than what is allowed by congestion control algorithm, and yet when the send window size reduces it is treated as if its size did not change.

  Conditions: The symptoms are observed at any time when congestion control is not disabled and the congestion window changes its size due to a change in network latency or processing rate.

  Workaround: There is no workaround other than disabling congestion control.

- CSCsk26165

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

  Conditions: The router must be configured for L2TP.

  Workaround: There is no workaround.

- CSCsk28361

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

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

  Workaround: There is no workaround.

- 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.

- CSCsk33724

  Symptoms: Starting with Cisco IOS Release 12.2(33)SXH, DOM feature is not 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 and later releases.

  2. Transceivers listed as "unsupported" in output of **show interface transceiver supported- list** command.

  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.

- CSCsk39022

  Symptoms: Broadcast may not be forwarded between VLANs.

  Conditions: The symptom is observed only on Modular IOS. It is seen with Cisco IOS Release 12.2(18)SXF10, when executing the command **ip directed-broadcast**.

  Workaround: There is no workaround.

- CSCsk39806

  Symptoms: The command **show bgp all dampening parameters** does not show the VPNv6 unicast address-family. Also, the VPNv6 address family may not be seen in the running configuration.

  Conditions: The symptom is observed when using Cisco IOS Release 12.4(20)T and when using the command **show bgp all dampening parameters**.

  Workaround: There is no workaround.

  Further Problem Description: The output of **show bgp vpnv6 unicast all dampening parameters** works properly. The impact of this issue is primarily display/UI.

- CSCsk39926

  Symptoms: FTP transfer fails if source interface is part of VPN routing/forwarding (VRF).

  Conditions: Occurs when the interface configured in **ip ftp source-interface** <*interface-name*> is part of a VRF or the FTP server is part of a VRF.

  Workaround: Use an interface that is not part of a VRF, and the FTP server should be known via global routing table.

  Further Problem Description: FTP client is not VRF aware. It always looks in the global routing table to reach the specified FTP server. If the specified FTP server is not known via the global routing table, the connection attempt will fail, either with a time out or destination unreachable error.

- 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.

- CSCsk43745

  Symptoms: The multicast switching path might be incorrectly displayed as fast- switched in the output of the **show ip interface tunnel x** command.

  Conditions: This symptom is observed when the **tunnel-sequence datagrams** command is enabled on the tunnel interface, which should disable fast-switching.

  Workaround: This is just a display issue. No workaround is needed.

- CSCsk49705

  Symptoms: The **ip nat inside source static network** command does not have the <cr> option.

  Conditions: This symptom is observed on a Cisco 7200 router that is loaded with Cisco IOS Release 12.4 or 12.4T.

  Workaround: There is no workaround.

- 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.

- CSCsk54092

  Symptoms: Link-state advertisement (LSA Type 3) may not get flushed from the database when the route is suppose to be included as LSA Type 5.

  Conditions: This symptom is observed when an LSA is changed from type 3 to type 5 on a Cisco router. This is a timing problem between OSPF and BGP. Routes redistributed into OSPF are shown as Type 3 LSAs when the **sh ip ospf <process-id> database** command is entered, even after the removal of the **network** command under the router which is advertising these routes. These routes are to be learned via Type 5 LSAs. This problem exists in all branches except Cisco IOS Release 12.2S.

Workaround: Configuring the PE routers in different domains using the **domain-id A.B.C.D** command can solve the issue.

- 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.

- CSCsk63794

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

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

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

- CSCsk64158

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

  Cisco has released free software updates that address this vulnerability.

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

- 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: 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.

- CSCsk65460

  Symptoms: Multicast fast switching fails on the decapsulating provider edge (PE) router when encryption is configured.

  Conditions: This happens on a Cisco 7200 router with Cisco IOS Release 12.4(17.4)T1.

  Workaround: There is no workaround.

- CSCsk66339

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

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

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

- 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. This problem occurs when msdp timer is set to 1.

  Workaround: There is no workaround.

- CSCsk68846

  Symptoms: Router Crashed when removing grandchild policy

  Conditions: Seen on a Cisco 7304 Router.

  Workaround: There is no workaround.

- CSCsk71117

  Symptoms: The topo_name on the upgraded version remains null, causing XDR to become disabled. All features that use XDR as their distribution mechanism will not work.

  Conditions: Software upgrade (ISSU) from SB9 to SR, that is, from pre-MTR release to post-MTR release.

  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.

- CSCsk75986

  Symptoms: A multilink bundle may go down when ACFC and PFC configurations are applied.

  Conditions: The symptoms are observed under a multilink interface on CPE and virtual-template on LNS.

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. The 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 .

- CSCsk81396

  Symptoms: Bus Error Exception at "sock_tcp_directwakeup."

  Conditions: Occurs on a Cisco WS-C6513 running Cisco IOS Release 12.2(18)SXF8.

  Workaround: There is no workaround.

- 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.

- CSCsk84925

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

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

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

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

  Workaround: There are several possible workarounds to this issue:

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

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

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

- 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.

- CSCsk86150

  Symptoms: When EIGRP goes down, BGP installs the major network in the routing table. When EIGRP comes up again, it installs the subnet routes in the routing table, while the BGP major network remains in the routing table. Also, the BGP local source route is not installed in BGP table.

  Conditions: Occurs on routers running Cisco IOS Release 12.4(10b) and 12.4(13c) Enterprise Services images.

  Workaround: Reconfigure the network command

- CSCsk86381

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

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

  Workaround: There is no workaround.

- CSCsk86642

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

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

  Workaround:

  1) **hw-slot reset** on the Sip400-SPA corrects the problem.

  2) A **shut/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.

- CSCsk89546

Symptoms: OSPF routes are not populated in the Routing Information Base (RIB) with the next hop as traffic engineering (TE) tunnels.

Conditions: Occurs when multiple TE tunnels are configured and the tunnels come up or are shut/no shut simultaneously.

Workaround: Shut/no shut tunnels one at a time.

- CSCsk91176

  Symptoms: When the crashinfo is being written to a disk, the IPC timeout messages is displayed, and line cards are reset.

  Conditions: This problem occurs on Cisco 10000 PRE3 and PRE4 when crash file is being written.

  Workaround: There is no workaround.

- CSCsk91267

  Symptoms: There are two symptoms:

  1. When you reset a WS-X6708-10GE card, you may see the following message:

  ```
  %OIR-SW2_SP-6-PWRFAILURE: Module 3 is being disabled due to power converter failure
  0x3
  ```

  2. When you turn off a power supply or due to a temporary power supply glitch, user may see a similar message:

  ```
  00:09:16: %OIR-SP-6-PWRFAILURE: Module 1 is being disabled due to power convertor
  failure 0xF
  ```

  OR

  ```
  %OIR-SP-6-PWRFAILURE: Module 2 is being disabled due to power convertor failure 0x8
  ```

  When you turn on a power supply, you do not see "power supply 1 online" message.

  Conditions: Occurs when a WS-X6708-10GE card is reset or when power is interrupted.

  Workaround: There is no workaround.

- CSCsk92854

  Symptoms: Traceback may be seen while testing L2TP scaling 32k functionality on a Cisco 10000 series router.

  Conditions: The symptom is seen with scaling scenarios and with a Cisco 10000 series router.

  Workaround: There is no workaround.

- CSCsk93241

  Cisco IOS Software Multi Protocol 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

- CSCsk94179

  Symptom: Connectivity problems are observed for IPv6 client, which obtained IPv6 prefix via DHCP for Virtual Access interface, due to incorrect static routes in the routing table for the assigned IPv6 prefix.

  Conditions: Occurs with IPv6 prefix delegation via DHCP, when client moves from one interface to another.

  Workaround: None

Further problem description: When IPv6 prefix delegation assigns a prefix for Virtual Access interface, it creates a static route for the prefix in the routing table. When a client moves to a new interface, old binding and the old routes are retained, which causes the problem.

- CSCsk95969

  Symptom: A HA router in SSO mode with both IPv6 unicast and IPv6 multicast configurations may crash while configuring IPv6.

  Conditions: The symptoms is observed on an HA router in SSO mode with both IPv6 unicast and IPv6 multicast configurations, when both configurations are removed completely and then configured again.

  Workaround: There is no workaround.

- 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.

- CSCsk98507

  Symptoms: Router crashes after IPX routing is enabled.

  Conditions: Problem happens only if an interface which has IPX network configuration is deleted after disabling IPX routing.

  Workaround: There is no workaround.

- CSCsk98751

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

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

  Workaround: There is no workaround.

- CSCsl01595

  Symptoms: Crash seen on Sup720 and RSP720 upon creating port-channel using range command. Crash not seen on Sup32.

  Condition: This problem will happen if a deleted port-channel interface on a Cisco 7600 is recreated through interface range command.

  Workaround: There is no workaround. As a solution, disabled creation of port-channel through interface range on the Cisco 7600.

- 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.

- 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 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
```

- CSCsl04415

  Symptoms: In a scale BGP IPv6 (more than 500 VRFs), setup with redistribution enabled, during bootup the CPU will be hogged. The BGP neighborhood will not be able to established.

  Conditions: Occurs under the following scenario:

  1. scale setup 2. BGP IPv6 3. redistribution enabled.

  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.

- CSCsl13561

  Symptoms: Enhanced EasyVPN will not pass traffic from inside interfaces over the IPSec tunnel.

  Conditions: Packets sent to or from the router will still pass correctly.

  Workaround: Configurations that do not require Enhanced EasyVPN features can downgrade to legacy VPN with no VTIs. If Enhanced EasyVPN features are needed, there is no work around.

- CSCsl13950

  Symptoms: The IPC port open failures.

  Conditions: The IPC port open failures due to very high CPU utilization (on both RP and RRP) during initialization. This is depending of the size of configuration file, for example when there are many ACLs.

  Workaround: There is no workaround.

- CSCsl14450

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

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

  Workaround: There is no workaround.

- CSCsl17798

  Symptoms: Etherchannel membership on standby supervisor inconsistent with the state on active supervisor. Reported in ESM-20G line card, possibly affecting traffic forwarding.

  Conditions: This defect may be seen with etherchannel mode is "on" after a standby reload. Reported in Cisco 7600 series router. Could impact other platforms as well.

  Workaround: Once standby supervisor has reached hot, remove etherchannel configuration and reapply. No other workaround exists.

- 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.

- CSCsl19708

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

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

  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 sub- interface 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.

- CSCsl21948

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

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

  Workaround: There is no workaround.

- CSCsl22080

  Symptoms: WebVPN hangs after a few days of working. When this happens, no WebVPN connections are active and no new connections can be established. The **debug ip tcp transaction** command shows **connection queue limit reached: port 443** errors. The **show tcp brief** command displays many sessions in SYNRCVD and TIMEWAIT states. Problem is recovered either by reload or by entering the **clear tcp tcb *** command. There are few stale sessions in CLOSED state left after clearing TCP.

  Conditions: Issue seen in Cisco IOS Release 12.4.15T and Cisco IOS Release 12.4.15T1 when WebVPN is configured. The issue is intermittent and happens after few days or weeks of working.

  Workaround: To restore TCP connectivity, issue **clear tcp tcb *** or reload the router. Note that this will clear all TCP sessions on the router.

- CSCsl23306

  Symptoms: The standby RP or standby SP may crash.

  Conditions: The symptoms are observed when the RP's 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.

- CSCsl26740

  Symptoms: Router crash when traffic engineering (TE) tunnels are removed.

Conditions: Occurred 600 TE tunnels were removed at once.

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.

- CSCsl28246

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

  Conditions: This symptom is observed under TC sessions.

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

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

  ```
  Nov 13 11:00:56.696 EST: %IDMGR-3-INVALID_ID: bad id in id_get (Out of IDs!)
  ```
  AAA is allocating only 1024*32 = 32,768 IDs. Not able to bring up any more sessions because of accounting flow ID allocation failure.

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

- 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.

- CSCsl28931

Symptoms: On Cisco 7600 configured with VPLS, if the traffic on the ingress direction and egress direction follows different Forwarding Engines (DFC or CFC), the dynamically learned entries may not be synchronized after a line card online insertion and removal (OIR), resulting in the traffic being flooded for those MAC entries.

Conditions: Occurs under the following scenario:

1. The traffic flow needs to be asymmetrical, for example in a VPLS scenario, the ingress traffic comes from a switchport in a ES-20 linecard (which has a distributed forwarding engine) and is forwarded to a core facing linecard like SIP-400. In this flow, the ingress traffic is forwarded by the ES-20 local forwarding engine and the opposite traffic (MPLS core to access) is forwarded by the central forwarding engine.

2. A line card OIR happens

Workaround: Clear MAC address table dynamic entries.

- CSCsl30331

  Symptom: 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.

- CSCsl31182

  Symptoms: The router experiences high CPU.

  Conditions: This issue only occurs when there is temporary Mroute inconsistency between PIM neighboring routers.

  Workaround: Enable **no ip pim v1-rp-reachability** on PIM-RP and non-RP PIM routers.

  Further Problem Description: The PIMv1 RP-reachability packet forwarding loop occurs when received from (*,G)'s non-RPF interface.

- 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

- CSCsl32122

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

  Conditions: Conditions are unknown at this time.

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

- CSCsl34481

  Symptoms: Router crashes due to IPv6 multicast routing.

  Conditions: This happens after applying multicast routing configurations, and again while unconfiguring.

  Workaround: There is no workaround.

- CSCsl34523

Symptom: 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.

- CSCsl36241

  Symptoms: The standby RP/SP running Cisco IOS Release 12.2(33)SRB gets reset continuously during the ISSU operations when the active RP/SP is running Cisco IOS Release 12.2(33)SRC.

  Conditions: It happens during ISSU loadversion or runversion operations if the configuration contains anything over MPLS (AToM) configuration.

  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.

- CSCsl39130

  Symptoms: Spurious memory access is seen while establishing L2TP tunnel (PPPoE-relay). The tunnel is never established.

  Conditions: Occurs on routers running Cisco IOS Release 12.4(18.2)PI1 when configuring L2TP active discovery relay for PPPoE and establishing PPPoE sessions from client.

  Workaround: There is no workaround.

- CSCsl39860

  Symptoms: Standby SUP keeps rebooting with stateful switchover (SSO) after running some SNMP CLI commands.

  Conditions: The following sequence of commands result in this issue.

  1. Execute the following CLI commands on the switch:

  snmp-server host <a.b.c.d> public

  snmp mib notification-log default

  snmp mib notification-log globalsize 10001

  snmp mib notification-log globalsize 10000

  2. Execute SSO. The standby will continue to reboot.

  Workaround: Do not use notification log MIB

- CSCsl40687

  Symptoms: Router reloads due to a bus error. This occurs with the following messages:

```
%ALIGN-1-FATAL: Illegal access to a low address 08:32:13 AEST Tue Nov 20 2007
addr=0xB8, pc=0x40099888 , ra=0x44020000 , sp=0x465870E8
08:32:13 AEST Tue Nov 20 2007: TLB (store) exception, CPU signal 10, PC = 0x40099888
-Traceback= 0x40099888 0x402F6358 0x415102F4 0x41510C7C 0x402FF5C4 0x414F1140
0x402FF7B8 0x41C8B8E0 0x41C8EFC0 0x41C8F064
0x41C85260 0x421EA0C4 0x421EA224
```

Conditions: This occurs after applying a Modular Quality of Service Command-Line Interface (MQC) class on a PVC.

Workaround: Use frame relay traffic shaping (FRTS) instead of MQC under the PVC.

Further Problem Description:

MQC policy is not a supported configuration for MLPoFR connections. The above configuration is not valid. Currently, the MQC policies are configurable under MLPoFR PVCs and this results in router reload. However, the router should not crash even under those circumstances. This fix prevents MQC QOS policy from being configured on MLPoFR connections at config time when MLP may not yet be active. So, in effect, the config is blocked both if MLP is active or if MLP is just configured.

- CSCsl40705

  Symptoms: The following tracebacks may occur on a VPDN under stress situations:

  ```
  %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
  ```

  Conditions: The symptom is observed in stress situations when a Call Disconnect Notification (CDN) is received immediately after a connect request.

  Workaround: There is no workaround.

  Further Problem Description: This traceback is harmless.

- 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.

- CSCsl41685

  Symptoms: Attaching a hierarchical policy with 250 classes to a switchport of an ES-20 fails.

  Conditions: Occurs with scaled configuration with 250 classes, with a child policy in class-default.

  Workaround: There is no workaround.

- CSCsl43546

  Symptoms: On the Cisco 7600, 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 occurs on the Cisco 7600 by issuing this command **hw- module** *module-number* **reset**.

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

- 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.

- 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.

- CSCsl44236

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

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

  Workaround: There is no workaround.

- CSCsl44497

  Symptoms: Unable to configure class parameters under policy-map.

  Conditions: Occurs after attaching service policy to any interface. If you try changing the class parameters, it will not enter into class configuration mode.

  Workaround: Detach the service-policy from interface and modify class parameters and attach it back to the interface.

- CSCsl46499

  Symptoms: When user configures service instance under port-channel interface and if the encap dot1q tag has the same value as the internal VLAN number of the main port-channel interface, then following error will show up:

  ```
  Nov 21 05:14:07.814: %GENERAL-DFC7-2-CRITEVENT: ETHER EFP CLIENT: Could not add qinq
  ```

Conditions: This happens when a service instance configured under port channel interface has the same “ecnap dot1q” tag value as the internal VLAN of the main port channel interface.

Workaround: There is no workaround.

- CSCsl46959

  Symptoms: The router may hang and not be recoverable when reloaded with a specific configuration.

  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.

- 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.

- CSCsl47613

  Symptoms: Services defined in the user-profile may not be applied to the session.

  Conditions: The symptom is observed when applying a service from the user- profile using Transparent Autologon with Autologon attribute A*service*.

  Workaround: Apply services using the service-profile, instead of defining them in the user-profile.

- CSCsl48075

  Symptoms: The floating static route behaves incorrectly in a v6 VRF. In a situation where there are two static routes via different interfaces in a v6 VRF and the Administrative Distance (AD) of one route is increased (floating static route), instead of installing the route with lesser AD as expected, the route with higher AD is installed in the routing table.

  Conditions: The symptoms are observed when there are two static routes via different interfaces in a v6 VRF and the AD of one route is increased.

  Workaround: There is no workaround.

- CSCsl48153

  Symptoms: When the CNS image retrieve operation is performed, the router may not download the associated image from the image server.

  Conditions: The symptom is observed when Image Server holds a valid image for the device.

  Workaround: There is no workaround.

- CSCsl49124

  Symptoms: TCAM debug messages are displayed.

  Conditions: Occurs while router is booting.

  Workaround: There is no workaround.

- CSCsl49167

Symptoms: Continuous %IPC-5-WATERMARK: 884 messages pending in xmt for the port slot on a Cisco 7600 SIP-400. It affects any type of Cisco 7600 chassis and is not specific to any supervisor. The messages are warnings that the buffer is being used up.

Conditions: The problem occurs under high traffic conditions between RP and line card. The underlying Ethernet Out of Band Channel (EOBC) transport encounters lots of collisions, which results in the WATERMARK message.

Workaround: There is no workaround.

- CSCsl49628

  Symptoms: When a VPN routing/forwarding (VRF) is deleted through the CLI, the VRF deletion never completes on the standby RP, and the VRF cannot be reconfigured at a later time.

  Conditions: This symptom is observed when BGP is enabled on the router.

  Workaround: There is no workaround.

- CSCsl49705

  Symptoms: ISSU between SRB-2 & SRB-3 done, with tunnels configured on active, causes "IDBINDEX_SYNC-4-RESERVE" messages on standby (SRB-2) & a delay (wait) of around 3 sec per tunnel. This causes a standby reset in cases where there are large number of tunnels configured.

  Conditions: Occurs when tunnels are configured.

  Workaround: Remove tunnel configurations before doing ISSU.

- CSCsl50271

  Symptoms: An Open Shortest Path First (OSPF) enhancement, to avoid a suspend when link state update packets are sent, may result in a router crash.

  Conditions: The symptoms are observed in a scenario with 3k tunnels. Both unconfiguring the loopback interface and deleting the loopback interface trigger the same code path that may lead to OSPF suspension.

  Workaround: There is no workaround

  Further Problem Description: The problem actually exists in all branches. However, this is a timing issue.

- 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.

- CSCsl50500

  Symptoms: System reset due to WATCHDOG ERROR.

  Conditions: Occurred during heavy stress condition CPU freeze observed. Specific to RSP720 hardware. Occurred only once and considered to be rare.

  Workaround: There are no workarounds that would guarantee that the problem will not occur. The probability of the occurrence can, however, be lowered by protecting the RP CPU from overload. This can be achieved by enabling MLS rate-limiters or configuring Control Plane Policing.

- CSCsl50569

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

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

Recovery: To recover connectivity, there are two options. Option 1 is preferable since it causes less traffic interruption. If Option 1 does not work, then Option 2 should be performed. 1. Attach to the switch processor (**remote login switch**) and issue the command: **test fpoe index 0 FFFF restore** 2. Reload the ingress SIP-400 linecard: **hw-module module** *mod* **reset**

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

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

- CSCsl50774

  Symptoms: Linecard crashes repeatedly during boot after an unsuccessful FPD upgrade.

  Conditions: Affects Cisco IOS Release 12.2SRB and will prevent the linecard from booting

  Workaround: There is no workaround.

- CSCsl51380

  Symptoms: Sup720 has periodic consistency checker for TCAM and SSRAM, from shadow to hardware which write to hardware when an inconsistency is detected between shadow and actual hardware. However, on a Sup720 and a Sup32 there is no verification to check whether the write was successful, and no syslog or notification is given to notify persistent hardware entry failures.

  Conditions: The symptoms are observed on a Sup720 and Sup32.

  Workaround: There is no workaround.

- CSCsl51395

  Symptoms: The device crashes when **hw-module reset** issued for the 6748 DFC card. Port Manager Internal Software Error and tracebacks are also consistently seen with the line card when **shut/no shut** or **Hw-module reset** was issued.

  Conditions: Applies to Cisco IOS Release 12.2SX and related releases.

  Workaround: There is no workaround.

- 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.

- CSCsl51765

  Symptoms: The router crashes on entering the **no t1 channel-group** command.

  Conditions: Occurs when the command is issued on a CT3 SPA on a SIP-400

  Workaround: There is no workaround.

- CSCsl51848

  Symptoms: Router crashes when a command is entered from the aux console to remove an interface.

  Conditions: Occurs when a **show command** for that interface is presently paused at the "more" prompt on the main console. The show commands are "show controllers serial" and "show interface serial".

Workaround: Avoid configuration while "show" commands are being run on the router.

- CSCsl51914

  Symptoms: On Cisco 7600/SIP400 supporting MLP interfaces, "priority percent" does not work.

  Conditions: The conditional police rate values won't get updated:

  1) Whenever a member link addition or deletion happens from the bundle.

  2) When all the members of the multilink are down and come back.

  3) SPA / LC online insertion and removal (OIR).

  Workaround: Use priority and with absolute-value (explicit) policer.

- CSCsl51945

  Symptoms: The HSRP IPv6 config on the standby RP may lose its address, such that the configuration 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.

  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 linecard 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.

- CSCsl52323

  Symptoms: In a scale configuration environment, anything over MPLS (AToM) manager signals RF bogus RF_DONE event.

  Conditions: This can result in a high availability misbehavior.

  Workaround: There is no workaround.

- CSCsl52508

  Symptoms: Keepalive tunnels for manual L2TP sessions fail to come up.

Conditions: This problem occurs when keepalive tunnels are configured for manual L2TP sessions.

Workaround: There is no workaround.

- CSCsl52594

  Symptoms: When two routers are configured to form an IPv6 EIGRP adjacency, attempts to ping one of the loopback IPv6 addresses from the neighbor fails with the following error:

  No valid source address for destination

  Conditions: Occurs on routers running Cisco IOS Release 12.4T.

  Workaround: There are two workarounds:

  1. Disable IPv6 Cisco Express Forwarding (CEF) 2. Enter the **clear ipv6 eigrp neighbor** command

- 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.

- CSCsl54243

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

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

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

  1. Configure a VLAN subinterface on an SPA.

  ```
  7600(config)#int gi 2/0/0.100
  7600(config-subif)#encap dot1q 100
  ```

  2. Physically insert another SPA into the SIP-400.

  3. Unconfigure the subinterface and observe the SIP-400 crash.

  ```
  7600(config)#no int gi 2/0/0.100
  ```

  Workaround: There is no workaround.

- 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.

- CSCsl55219

  Symptoms: VFI manager process thrashing occurs when a core interface flaps.

  Conditions: When core interface flaps, VFI manager process thrashing occurs, as VFI manager is not returning when the bulk sync is done.

  Workaround: There is no work around

- 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.

- CSCsl56824

  Symptoms: STP does not block a port and creates network loop after reload PE router.

  Conditions: This problem is observed when using Virtual Private LAN Services (VPLS).

  Workaround: There is no workaround.

- CSCsl56934

  Symptom:

  "ip summary-address rip" is configured on an interface, but the summary address is not advertised by RIP.

  Conditions: Occurs, after the same interface was deleted and re-created with "ip summary-address rip" configured on it (e.g Virtual Access interface or Loopback). Originally observed when connecting and disconnecting virtual access sessions. The issue is platform-independent.

  Workaround: None

- CSCsl57023

  Symptoms: PVC recreation may fail after a switch-over occurs on a Cisco 7600 series router and a new active is reset.

  Conditions: The symptom is observed when a switch-over occurs on a Cisco 7600 series router from active to standby.

  Workaround: There is no workaround.

- CSCsl57457

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

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

  Workaround: There is no workaround.

- CSCsl59629

  Symptoms: SNMP walk gets stuck in infinite loop.

  Conditions: Occurs while doing snmpwalk for ciscoFlashMIB.

  Workaround: There is no workaround.

- CSCsl60092

  Symptoms: Router crashes as the client is trying to return a fragmented message but not the last fragment.

  Conditions: Seen on a system running stress test with Layer 3 unicast/multicast and Layer 2 traffic with 5K OSPF, 20K BGP routes, 10K IGMP groups, 98K mac addresses. Running a script to **shut/no shut** VSL control port every 5 seconds and wait 10 seconds between different ports on both the active and the standby, the crash was seen on active SP about 3 hours into the test.

  Workaround: There is no workaround.

- CSCsl60107

  Symptoms: VPLS/EoMPLS traffic may be dropped at imposition when a Weighted Random Early Detection (WRED) policy applied to any port on the same hardware datapath on SIP-600 or ES-20. 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 a router with scaled QoS configurations, the OSM line card may suffer memory fragmentation errors.

  Conditions: Occurs with QoS with scaled configurations.

  Workaround: There is no workaround.

- CSCsl61164

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

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

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

- CSCsl61806

Symptoms: When the sum of EIRs of all BW queues under an ESM20 linecard exceeds 549Gbps, the following message may be produced: "EXCEEDEXCESSQRATE".

Conditions: The symptom is observed in an environment which has a large configuration with 1000 EVCs with WRED-configured policy maps under a PC interface. When the WRED is removed from a class which has a shape rate, a number of exceed excess error messages are seen. When the **shutdown** command is executed followed by the **no shutdown** command on the PC interface, most of the queues go to pending state with the exceed excess error message flooding the screen.

Workaround: Changing either the shape rate or adding the WRED back to the class-map will resolve the problem. Reloading the linecard will also recover this problem.

- 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.

- CSCsl62341

  Symptoms: The configuration command **ip summary-address rip** is not applied by radius configuration as part of the lcp:interface-configuration.

  Conditions: This symptom is observed only when the lcp:interface- configuration is used in combination with other AVPairs that perform an interface-specific configuration. For example, the last four AVPairs shown below use a mix of lcp:interface-configuration and interface-specific AVPairs: xxxxx@xxxx2001 Password = "xxxx" Service-Type = Framed-User, Framed-Protocol = PPP, Framed-IP-Address = 10.17.1.1, Framed-Routing = listen, av-pair = "ip:description=sub-VAI ppp1", av-pair = "ip:vrf-id=X2001", av-pair = "ip-unnumbered=Loopback2001", av-pair = "lcp:interface-config=ip summary-address rip 10.17.1.0 255.255.255.0"

  Workaround: If you require a summarized address to be advertised via RIP to CPEs, ensure that the lcp:interface-configuration command/attribute is used for all interface specific configurations, as this issue occurs when the interface specific commands/attributes are mixed between the AVPairs and the lcp:interface-configuration commands. The interface profile should be applied before applying any IP configuration profiles.

- CSCsl62344

  Symptoms: If a contact phone number is configured to be 12 digits long, the configuration will fail. If the configuration is already in the running- configuration, the call-home configuration will lost after reload.

  Conditions: The symptom is observed when the call-home contact phone number is configured to be 12 digits long.

  Workaround: Add a white space in the contact phone number to make it at least 13 digits long.

- 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.

- CSCsl62963

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

Conditions: Seen on a Cisco 7200 router.

Workaround: There is no workaround.

- CSCsl63212

  Symptoms: L2TP network server (LNS) router crashes while establishing virtual private dial-up network (VPDN) and shutting down client interface.

  Conditions: Occurs while making call from client to LNS with specific configurations.

  Workaround: There is no workaround.

- CSCsl63311

  Symptoms: On a Cisco Catalyst 6500 Series Switch, NAT traffic may be software switched. This may result in high CPU utilization.

  Conditions: The symptom is observed when the NAT traffic egress on an interface is configured as an ISL L3 sub-interface.

  Workaround: Use DOT1Q instead of ISL.

  Alternate Workaround: Make the connection a Layer 2 ISL trunk and create an SVI for each sub-interface.

- CSCsl63494

  Symptom:

  AAA server does not count active user sessions correctly. User authentication may be denied by the AAA server because max session limit has been reached.

  Conditions:

  This may occur with AAA authentication, when max session limit is configured on Cisco Secure ACS server (may happen with other AAA servers too). When user initiates X.25,ssh,rsh,rlogin or telnet sessions and later disconnects them, AAA server does not decrement active sessions counter due to wrong attributes present in the accounting records sent by the device. Eventually, the misbehaving counter may reach max session limit, and user will be denied a login.

  Workaround: Removing max session limit can be considered.

- CSCsl64890

  Symptoms: Ping fails for packet sizes greater than 1500.

  Conditions: Applicable to RSP720 supervisor and with Filer Feature in Cisco IOS Release 12.2(33)SRC. This bug is not applicable to any other releases.

  Workaround: There is no workaround.

- CSCsl65047

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

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

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

- CSCsl65087

  Symptoms: SIP200 linecard crashes due to memory corruption when high traffic passes through on a software based dLFI bundle which has ACFC/PFC configured.

Conditions: Happens when traffic on the bundle is oversubscribed.

Workaround: There is no workaround.

- CSCsl65179

  Symptoms: Setting priority queue limit for PFC QoS configurations resets non- priority queue limits to default values.

  Conditions: The symptom is observed when changing the priority queue limit for PFC QoS to the default setting. If CoS values are mapped to queues with default queue limits of zero, then traffic with these CoS values will be dropped until non-default configuration is reapplied.

  Workaround: After changing the priority queue limit, reapply non default non- priority queue limits.

  Further Problem Description: Setting the **priority-queue queue-limit** to the default values via the **no priority-queue queue-limit** or **default priority-queue queue-limit** commands sets the WRR queue limits to default values. This action has the side effect of dropping all traffic mapped to queues 4 and 5 until the WRR queue limits are reconfigured.

- 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.

- CSCsl65407

  Symptom: 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.

- CSCsl65820

Symptoms: BGP backdoor functionality is not working.

Conditions: This symptom occurs after using the **clear ip bgp *** command.

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

- 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.

- 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: 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.

- 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.

- CSCsl70175

  Symptoms: A router running Cisco IOS may crash if a sequence of configuration commands like the following is entered at the prompt:

  router eigrp 101 redistribute bgp 300 router eigrp 101 redistribute bgp 200

  The crash is not specific to redistribution commands under EIGRP; entering two **redistribute bgp <AS>** commands with different AS numbers anywhere could trigger the crash.

Conditions: BGP does not have to be running prior to the **redistribute bgp <AS>** configuration commands being entered. The crash is not specific to any other routing protocol, so entering two BGP redistribution commands with different AS numbers anywhere on the router can trigger the crash.

Workaround: Check configurations before applying them to the router to be sure that the AS numbers used for all redistribution commands are correct.

- CSCsl70343

  Symptoms: When Ethernet CFM is enabled and MEP is configured on a router, it does not learn the remote MEPs.

  Conditions: No output is shown when the **show ethernet cfm maintenance-points remote level 5** command is entered.

  Workaround: There is no workaround.

- CSCsl70408

  Symptoms: During the active & stand-by PRE synchronization on Cisco 10000, stand-by PRE encounters CPU hogs which eventually results in active resetting the stand-by. Standby displays the following message:

  ```
  *Oct 16 07:43:00: %SYS-3-CPUHOG: Task is running for (6000)msecs, more than
  (2000)msecs (2/2),process = BEM VERIFY
  ```

  Conditions: Occurs on a Cisco 10000 (PRE-2/PRE-3) with a large (2mb+) configuration and configured for stateful switchover (SSO).

  Workaround: Disable/remove the standby PRE.

- 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.

- CSCsl70722

  Symptoms: A router running Cisco IOS may crash due to watchdog timeout.

  Conditions: Occurs when IP SLA probes are configured and active for a period of 72 weeks. After this much time has passed, polling the rttmon mib for the probe statistics will cause the router to reload. Then the problem will not be seen again for another 72 weeks.

  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.

- CSCsl70963

  Symptoms: Whenever there is member link updates and/or parent class policy-map modification which involves bandwidth change, the bandwidth change will not be reflected on the SIP2 linecard.

  Conditions: The symptom is observed on any hardware switching platform/linecard, such as SIP-400.

Workaround: Use priority and with absolute-value (explicit) policer.

- CSCsl71254

  Symptoms: A Cisco 7609-S with RSP720 processor, using ES20 line card, and running Cisco IOS Release 122-33.SRB2 crashes.

  Conditions: Occurs when configuring L3 subinterface with dot1Q NATIVE encapsulation on ES20 card interface, where already service-instance configured.

  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.

- 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.

- 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(32)SB or later releases, or Cisco IOS Release 12.2(32) SRB or later releases, that is configured for Stateful-Switchover (SSO) and Nonstop Forwarding (NSF).

  Workaround: There is no workaround.

- CSCsl72774

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

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

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

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

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

- CSCsl72789

  Symptoms: SW_INIT_TIMEOUT message for ES20 line cards, line card may or may not recover.

  Conditions: Generally this error is seen with large routing tables, large configurations with many subinterfaces, or in the case of hardware failure.

  Workaround: Depending on the source of the error, the workaround may be to reload the line card or reload the chassis. Some problems may have no workaround.

  Further Problem Description: This fix will effectively remove the possibility of a SW_INIT_TIMEOUT.

- CSCsl72826

  Symptoms: Router crashes at ipfib_policy_forward.

  Conditions: The issue seems to occur when a script is removing route map configurations and reconfiguring them at very short intervals. This occurred during internal testing and is not likely to occur in a production environment.

  Workaround: There is no workaround.

- CSCsl72831

  Symptoms: Cisco 7600 displays the following error:

  CWAN_CHOC_DSX-3-VC_CONFIG_ERR

  Conditions: Occurred while configuring channelized OC3 SPA on c7600-SIP-200.

  Workaround: There is no workaround.

- CSCsl74120

  Symptoms: Classification is broken after online insertion and removal (OIR) in Optical Services Module (OSM), as the OSM queues are not created.

  Conditions: Occurs after an online insertion and removal (OIR) event.

  Workaround: Remove and attach the policy again on the interface to 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. 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.

- CSCsl74712

  Symptoms: When an existing Virtual Router Redundancy Protocol (VRRP) tracking entry is re-entered into the configuration of the active RP, the standby RP automatically resets.

  Conditions: This problem only occurs after the following sequence of configuration events:

  - VRRP is configured to track an existing tracking object.
  - The existing tracking object is removed from the global tracking configuration.
  - The standby is initiated and establishes the full STANDBY state.

- The user re-enters the VRRP command to track the previously removed tracking object.
- At this point the Standby RP will reset due to PRC mismatch.

Workaround: During normal configuration it is unlikely that the above scenario will be repeated. Crucially the workaround for this defect is to make sure that when VRRP is using a tracked object, the global tracking config for that object must exist at all times. The global tracking config for that object can be removed as long as the tracking entry in VRRP is removed first.

- CSCsl74772

  Symptoms: Changing the shaping parameter not having an effect.

  Conditions: Occurred on a Cisco 7200 router configured with a three-level policy with shaping configured in parent level.

  Workaround: Remove the policy from the interface, modify the value, and attach it again.

- CSCsl75136

  Symptoms: Switch with Sup32 supervisor running modular Cisco IOS software may fail to boot up after a power cycle.

  Conditions: Occurs after the switch has been power cycled.

  Workaround: There is no workaround.

- CSCsl75257

  Symptoms: Virtual CEM interface remains down on the new active after switchover

  Conditions: Switchover from active to standby causes this problem on the new active.

  Workaround: Remove and recreate the virtual CEM interface by removing the **clock master/clock slave command** and reconfiguring it.

- CSCsl75960

  Symptoms: Cisco 7200 router crashes while reconfiguring IPv6 DHCP client pd.

  Condition: This happens on a Cisco 7200 router loaded running internal build of Cisco IOS Release 12.4.

  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.

- CSCsl76647

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

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

  Workaround: There is no workaround.

- CSCsl77385

  Symptoms: Long delay of RF_PROG_ACTIVE event was observed on Catalyst 6500. The delay caused anything over MPLS (AToM) VCs stay down after a switchover

  Condition: Occurs after system bootup with scale configuration.

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.

- 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 !
  ```

- 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 linecard reset may not come up.

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

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

- 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.

- 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.

- CSCsl80682

  Symptoms: VPN SPA crashes when encryption ACLs are modified.

  Conditions: Was seen happening when GRE takeover configured (GRE acceleration being done by SPA): **crypto engine gre vpnblade**

  Workaround: Configure GRE acceleration to be done by supervisor: **crypto engine gre supervisor.**

- CSCsl80870

  Symptoms: While bringing up 20 MLPoATM bundles with 10 member links, a few member links fail to come up.

  Conditions: This symptom occurs when some of the member links are inactive when the bundles come up.

  Workaround: There is no workaround.

  Further Problem Description: The cause for this issue is the bundle auth type does not match with the current links auth type. The current link name does not match the bundle first link name. CONFREJ is sent, and the member is removed from the bundle.

- CSCsl80887

  Symptoms: The router may crash and there is high CPU usage if the Routing Information Protocol's (RIP) minimum update interval is configured to zero.

  Conditions: The symptom may be observed on a Cisco router using RIP version 2 process, with the timer values set to 0 1 0 1.

  Workaround: Do not configure RIP's minimum update interval to zero.

- CSCsl81011

  Symptoms: Hierarchical queuing 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.

- CSCsl81012

  Symptoms: Cisco 7600 configured with SSO High Availability, with large number of EVC with bridge-domain, may experience a crash during bootup. Occurs while the standby supervisor is coming up.

  Conditions: This happens in the following conditions:

  - Cisco 7600 with dual supervisor in SSO redundant mode.

  - During bootup, after active RP booted and standby RP is coming up (HA syncing is happening).

  - LC reloads (which can happen when the card is first brought up during boot).

In the above case, the active may crash, which forces the standby to crash, since it has not been configured yet.

Workaround: Keep standby powered off until active and LCs come up and then power the active.

- CSCsl81243

  Symptoms: While provisioning the VC values in l2transport mode we were bringing up the vc-ckt in case of encapsulation mismatch. The bringing up of the circuit and encapsulation comparison was being done without checking if the other end of the l2trans ckt was of the same type in our case ATM. As a result the app_data of the other side which was being assigned as vc_info parameter created problem and led to the crash.

  Conditions: Occurs when end connection of l2trans ckt has different interfaces.

  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.

- CSCsl83212

  Symptoms: Traceback error message is shown every 10 seconds in the log on both Active and Standby RPs:

  ```
  *Dec 17 20:48:47.342: assert failure: NULL!=tinfo: ../const/common-
  rp/const_macedon_tunnel.c: 3875: macedon_tunnel_check_takeover_criteria *Dec 17
  20:48:47.342: -Traceback= 42C53118 42C59EB0 42C61938 42C621CC
  ```

  Conditions: This symptom is observed when an autotemplate interface is deleted from router configuration.

  Workaround: Recreating the same autotemplate interface that is being deleted will stop this traceback error message.

- 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.

- 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.

- 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.

- 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.

- 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.

- CSCsl86614

  Symptoms: E-OAM loopback session gets broken after SSO.

  Conditions: This issue is observed in the following scenario:

  1. Two routers are connected back-to-back and configured for e-oam.

  2. A remote loopback is created and then a switchover is performed.

  It is expected that the loopback status holds during switchover, however, the interface exits that state.

  Workaround: There is no workaround.

- 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.

- CSCsl87404

  Symptoms: L2TP tunnels are not getting established.

  Conditions: Occurs on a router running Cisco IOS Release 12.4(15)T2.

  Workaround: There is no workaround.

- CSCsl87843

  Symptoms: When changing the IP/IPv6 address of the interface, the Gateway Load Balancing Protocol (GLBP) operating on this router temporarily flaps to another GLBP group member.

  Conditions: The problem only occurs when the new IP/IPv6 address is lower than the existing address. The problem does not occur if it is higher. There must be more than one GLBP router in the group.

  Workaround: Do not change the IP/IPv6 address of the interface while the current router is actively operating as a member of a GLBP group.

- CSCsl87935

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

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

  Workaround: There is no workaround.

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

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

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

- 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.

- CSCsl89627

  Symptoms: Large packets may be dropped when running Bridge Control Protocol (BCP).

  Conditions: When BCP is under test, sweep ping fails when large tagged package is sent across the routers with BCP configured on serial ports. Specifically, for datagram sizes in the range [Min size=36, 1406] inclusive, ping goes through. But for larger datagrams in the range [1490 18024=Max Size] inclusive, the ping across the bridge fails.

  Workaround: There is no workaround.

- 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

  Symptom: 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.

- CSCsl91046

  Symptoms: Traffic coming into GigabitEthernet interface on OSM card is dropped on the line card.

  Conditions: On router boot-up, GigabitEthernet interface on the OSM card with scaled swEoMPLS configurations drops traffic that ingresses into the card. Transmit side, however works fine. Occurred on a router running Cisco IOS Release 12.2(33)SRC.

  Workaround: Use **shut/no shut** on the affected interface.

- CSCsl92316

  Symptoms: Router may experience mwheel CPUHOG condition.

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

  Workaround: There is no workaround.

- 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 Intermediate System-to-Intermediate System (IS-IS) VPN routing/forwarding (VRF) is configured. Bulk-sync failure due to PRC mismatch. The error can be seen by using the **show redundancy config-sync failures prc**.

  Workaround: There is no workaround.

- CSCsl93629

  Symptoms: FlexWAN linecard 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.

- CSCsl93767

  Symptoms: Dynamically updating an hierarchical queueing policy on a session may result in wrong traffic distribution to the classes.

  Conditions: The symptom is seen on a PPPoEoVLAN session using integrated hierarchical queueing (shaping policy on the VLAN, HQoS policy on the session) and when the parent policy on the session has "bandwidth remaining ratio" configured.

  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.

- 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.

- 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.

- CSCsl94499

  Symptoms: When applying the **mpls ip** under the top configuration mode command, the standby RP may be reset and the active RP generates the following error message:

  ```
  Dec 27 09:14:43.095 PST: %RTMGR-3-TOPO_SYNC_ERR: Failed to duplicate active topology
  on standby. (rc=15), id 1E000000 {default:ipv6:base}
  ```

  Conditions: The problem happens on a Cisco 7600 series router when applying the **no mpls ip** top configuration mode command.

  Workaround: Enable the IPv6 routing explicitly via the **ipv6 unicast- routing** command before issuing the **no mpls ip** command.

  Further Problem Description: There is a synchronization (or timing) issue on IPv6 routing shutdown between active and standby RPs.

- CSCsl94621

  Symptoms: For the ATM multi-VLAN to VC feature, when the remote end of the link flaps, the spanning tree instance for the VLAN gets lost, 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 linecard 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 linecard 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.

- CSCsl95609

  Symptoms: When a VRF which has BGP multipath that has been defined using the **address-family ipv6 vrf** *vrf-name* command is deleted, alignment tracebacks may be seen on the console.

  Conditions: The symptom is observed on a VPNv6 with BGP multipath defined.

  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.

- CSCsl96254

  Symptoms: If an EIGRP distribute-list that is applied to an interface allows a route, the route will be installed into the routing table without first checking to see if the global distribute-list allows it as well. All platforms are affected.

  access-list 1 permit any access-list 2 deny any

  router eigrp 1 network 192.168.1.0 0.0.0.255 distribute-list 1 in FastEthernet0/0 distribute-list 2 in no auto-summary

  The configuration above should deny all routes by virtue of access-list 2. Instead, all routes are allowed per access-list 1.

  Conditions: Running EIGRP with interface distribute lists and a global distribute list. All platforms are affected.

  Workaround: Currently the only workaround is to apply the global distribute list to each interface distribute list.

- CSCsl96335

  Symptoms: When a subscriber connects and disconnects from an ASR1000 at a high level of calls per second, the system may encounter an error with the following traceback:
  ASR1000-EXT-SIGNAL: U_SIGSEGV(11), Process = AAA SEND STOP EVENT

  Conditions: The symptoms are observed when an ASR1000 is functioning as LAC or LNS with ACL, QoS and uRPF features. AAA accounting is enabled for tunnel, sessions and PPP.

  Workaround: If the error is encountered persistently, consider disabling AAA accounting as temporary remedy.

- CSCsl96370

  Symptoms: A CPUHOG message may be seen.

  Conditions: This symptom is observed when the following three conditions are met:

  1. HSRP debugs are enabled.

  2. The router is logging to console.

  3. An interface with more than 50 HSRP groups is shut down.

  Workaround: There is no workaround.

- CSCsl96417

  Symptoms: Router crashes during ISSU upgrade.

  Conditions: Occurs during ISSU upgrade with ATM PVCs (configured with xconnect). The router crashes on running the ISSU runversion command.

Workaround: There is no workaround.

- 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.

- CSCsl97835

  Symptoms: The standby supervisor may crash.

  Conditions: Occurred in a system with scaled configuration with a operational rep segment. Occurred when a rep port role was configured as non-edge and then swapped to edge.

  Workaround: Shutdown the port before making changes described above.

- 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.

- 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.

- 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.

- CSCsl99629

  Symptoms: PIM hello packets are dropped and PIM neighbor is lost.

  Conditions: The problem happens when IGMP rate limiter is configured and global PIM snooping is turned on, such as in the following configuration:

  mls rate-limit multicast ipv4 igmp 500 100 ip pim snooping

  Workaround: There is no workaround.

- CSCsm00570

  Symptoms: FlexWAN card crashes after a service policy is attached to sub-interface in which mulitlink is configured, followed by **shut/no shut**.

  Conditions: This problem requires both a QoS configuration change and an interface flap to happen at the same time. It is not likely to happen in production environments.

  Workaround: There is no workaround.

- CSCsm00811

  Symptoms: In the following configuration

  TGN--------UUT1(atm4/0.1)---------(atm3/0.1)UUT2----------PKTS

  UUT2 hangs if IPv6 traffic is sent from TGN to PKTS through ATM subinterface.

  Conditions: Occurs when IPv6 CEF is enabled.

  Workaround: There is no workaround.

- CSCsm01126

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

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

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

  Workaround: There is no workaround.

- 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.

- CSCsm01389

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

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

  Workaround: There is no workaround.

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

- 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.

- CSCsm01509

  Symptoms: IP sessions fail to recover after a RP forced switch-over in SSO mode.

  Conditions: Problem can be observed after having both RP active and standby RP present in ACTIVE and STNADBY_HOT mode. All DHCP initiated ip-sessions are present, both active and standby RPs show the same number of sessions and DHCP binding.

  After a forced switchover, the following occurs:

  - The software allows learning (copying) of subscriber session information Active->Standby ONLY when the Standby is running and HOT;

  - Older IP sessions (IP sessions established before the standby became running and HOT) are NOT recognized by the NEW_Standby;

  - A trace back error is logged when the NEW_Standby has finished booting:

  ```
  %DATACORRUPTION-STDBY-1-DATAINCONSISTENCY: copy error, -PC= 0x0AB99EB0)
  -Traceback= 85C1990 85C209C 8524DB0 853C8A8 AB99EB0 AB93A18 AB9FC20 AB9DD3C AB9E024
  AB94254 AB94428 AB94580 AAA55F4 AA9B154
  ```

  Workaround: There is no workaround.

- CSCsm01577

  Symptoms: When an OC-3 CEoP SPA has a large IMA configuration, a SPA Online Insertion and Removal (OIR) will sometimes cause a number of groups to remain down. A SIP-400 OIR is required to bring the groups up.

  Conditions: The symptom is observed when OC-3 CEoP SPAs are configured with IMA in a back-to-back connection, and traffic is passing. In this situation, a SPA OIR will cause IMA groups to remain down.

  Workaround: Perform an OIR on the SIP-400.

- 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.

- 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.

- CSCsm06057

  Symptoms: c7600-SIP-400 stops forwarding traffic after RPR+ switchover

  Conditions: If the redundancy mode is RPR+ and after the switchover happens, traffic through the c7600-SIP-400 stops.

  Workaround: Reset the linecard using the **hw-module module <slot> reset**.

- 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:

  ```
  Jan 4 10:42:33.357 ROUTER: %IPRT-3-NDB_STATE_ERROR: NDB state error (BAD EVENT STATE)
  (0x00) 192.168.116.152/30, state 7, event 2->1, nh_type 1 flags 4 -Process= "RIP
  Router", ipl= 0, pid= 494
  ```

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

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

Workaround: The route can be restored by doing:

clear ip route 192.168.116.152

- CSCsm06769

  Symptoms: Cisco 7600 configured with service instance under the port-channel interface and channel-group <port-channel-number> mode on under the physical member, can experience a router crash if the member is unbundled via issuance of **no channel-group <port-channel-number> mode on**.

  Conditions: Occurs when port-channel with service instances, and at least one member port are unbundled using by removal of **channel-group** command.

  Workaround: There is no workaround.

- CSCsm08000

  Symptoms: A bridge-domain EVC is configured under port-channel interface. The EVC is in shutdown state, but the traffic still passes through the EVC.

  Conditions: This condition is hit when router boots up with the configuration where a bridge-domain EVC under port-channel is shutdown.

  Workaround: Toggle the admin state of the EVC by performing a **shut/no shut** under the service instance.

- CSCsm09338

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

  ```
  *Feb 1 19:46:32.132 buc: %C6K_PROCMIB-DFC7-3-IPC_PORTOPEN_FAIL: Failed to open port
  while connecting to process statistics: error code = no such port
  ```
  Conditions: 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 linecard.

- CSCsm09927

  Symptoms: Interface flaps continuously after running atlas BERT.

  Conditions: During atlas BERT another interface with lower anyphy number should be deleted.

  Workaround: Reload the shared port adapter (SPA).

- 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.

- CSCsm10603

  Symptoms: L2TP sessions flap both when idle and when traffic is being passed.

  Condition: Occurs on an internal version of Cisco IOS Release 12.4T only on the Cisco 1760 platform and while the voluntary tunneling feature is invoked.

  Workaround: There is no workaround.

- CSCsm12247

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

  Conditions: The router must be configured for WCCP redirection using the hash assignment method. When there is only a single appliance in the

  service group, the loss of hash assignment details is permanent.

  However with multiple appliances in the group, the loss of assignment information is transitory; the router soon recovers.

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

  Further Problem Description: 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 switchover, 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.

- CSCsm14007

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

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

  Trigger: Unknown.

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

  Workaround: There is no workaround.

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

- 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.

- CSCsm15350

  Symptoms: The VPNSPA may crash with an assert failure.

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

Workaround: There is no workaround.

- CSCsm15406

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

  Condition: 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.

- CSCsm17066

  Symptoms: One of the GLBP forwarders for a group may experience a state flap between two of the group members.

  Conditions: The symptom is observed after SSO occurs on a router in which the pre switch-over state for GLBP is "LISTEN". The forwarder which is assigned to this group member will experience the flap. It will only occur on setups where there are more than two GLBP group members.

  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.

- CSCsm19663

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

  Conditions: This symptom is observed with the following configuration:

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

  Workaround: There is no workaround.

- CSCsm20102

  Symptoms: Sending traffic at a rate of 70 percent across large number of Multilink PPP (MLPPP) bundles may result in a 0.4 to 2.5 percent loss of traffic.

Conditions: The symptom is observed when sending traffic at a rate of 70 percent across large number of MLPPP bundles with QoS and netflow configured. Traffic rate is well below the CFG drop rate(s) of the applied QoS policy. PXF counters and policy-map counters may also show drops. A reduced traffic rate (for example, 40 percent) may also show the same issue.

Workaround: Remove QoS policy or turn off netflow. Note: In both cases a write-mem/reload must be issued or cards must be reloaded using the **hw-module slot** *slot-number* **reset** command before changes will take effect.

Alternate Workaround: Reduce the number of MLPPP bundles.

Further Problem Description: It affects distributed platforms (Cisco 10000 series routers and others).

- CSCsm20599

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

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

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

- 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.

- CSCsm21126

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

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

  Workaround: There is no workaround.

- CSCsm21435

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

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

  Workaround: There is no workaround.

- 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.

- 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.

- CSCsm23764

  Symptoms: A device keeps reloading every 50 minutes.

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

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

  Impact: This issue affects operations.

  Workaround: Reload the active PRE if this issue occurs.

- CSCsm25854

  Symptoms: Dropped packets are not being counted for DLFI interfaces.

  Conditions: Occurs when DLFI is configured over Frame Relay, and policy map is attached to virtual template.

  Workaround: There is no workaround.

- CSCsm26130

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

  Conditions: This symptom is observed with auto-summary enabled in BGP. A static summary route is configured to null0 and is injected into the BGP table with a network statement.

  Workaround: There are four possible workarounds:

  1) Use an "aggregate-address" configuration instead of the static route to generate the summary. 2) Remove auto-summary from the BGP process. 3) Enter the **clear ip bgp *** command. 4) Remove and reconfigure the BGP network statement for the summary route.

- 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.

- CSCsm26610

  Symptoms: A router running Cisco IOS may unexpectedly reload.

  Conditions: This is specific to platforms with powerpc processors, such as the npe-g2 and 2600xm series routers. It requires either the legacy rate-limit config or MQC style policer configured on an interface.

  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:

  ```
  *Jan 18 05:44:07.880 GMT: %SYS-3-CPUHOG: Task is running for (2000)msecs, more than
  (2000)msecs (2/1),process = Exec.
  ```

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

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

- CSCsm27726

  Symptoms: After overwriting DHCP pool and client pool, status of client is IDLE.

  Conditions: Occurs on Cisco routers running a pre-release version of Cisco IOS Release 12.4(17b).

  Workaround: There is no workaround.

- 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.

- CSCsm29120

  Symptoms: PIM neighbor times out on interface that was once configured as port-channel. This happens for both IPv4 and IPv6 multicast. This issue is consistently reproducible. If PIM times out, multicast traffic will not flow on the interface.

  Conditions: Occurs under the following scenario:

  1. Configure port-channel on Ethernet interfaces.

  2. Configure IPv4 and IPv6 address on the port-channel interface. PIM neighbor will be formed.

  3. Remove Ethernet interface from the bundle interface and configure a IPv4 and IPv6 address. PIM neighbor will timeout after 1 minute 45 seconds.

  Workaround: Remove the interface from the port-channel, then perform a **shut/no shut**.

- CSCsm30569

  Symptoms: Packet is not being fragmented when packet size is greater than IPSEC tunnel MTU.

  Conditions: This issue is seen on routers running Cisco IOS Release 12.4T when IPSec is configured and Cisco Express Forwarding (CEF) is enabled. When CEF is disabled this issue is not seen.

  It occurs when packet size is greater than IPSec tunnel MTU. Packet is not being fragmented, however traffic is passing successfully.

  Workaround: There is no workaround.

- 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.

- CSCsm32392

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

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

  Workaround: There is no workaround.

- 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. The device could also experience High CPU in IP INPUT because of process switching all packets.

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

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

- 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.

- CSCsm36745

  Symptoms: SSM mapping may cause slow IGMP processing.

  When SSM Mapping for mapping IGMPv1/v2 reports to PIM-SSM is configured using **ip igmp ssm-map enable**, the IGMP process may slow down and not service all incoming reports and not send out periodic queries.

  Conditions: By default, when SSM mapping is configured, the router will try to resolve via DNS any mappings that are not statically configured. When the name server does not respond timely to the DNS lookups, which could be to non- or misconfiguration, name server down etc, other incoming IGMP reports will be delayed until the lookup has timed out. This also affects IGMP reports that are not supposed to be mapped.

  Workaround: - Create static mappings for all reports that are to be mapped - Make sure that all to be mapped IGMP reports are present in the configured name server - Disable DNS lookup using: **no ip igmp ssm-map query dns**

- CSCsm37834

  Symptoms: ES20 or SIP600 cards may reset with the following error:

  ```
  %EARL-DFC7-2-SWITCH_BUS_IDLE: Switching bus is idle for 5 seconds. The card grant is 0
  ```

  Conditions: The symptom is observed when performing an RPR switchover or "test crash" on the active supervisor. It is seen in HFS-enabled chassis (such as S-chassis or infinity chassis).

  Workaround: There is no workaround.

  Further Problem Description: The problem occurs because of a loss of synchronization on the switch fabric. This results in the loss of EARL heartbeat packets causing the EARL recovery process to complain that a bus stall has occurred when it finds that no heartbeat packets have been received.

- 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.

- CSCsm39002

  Symptoms: "Any-phy" of serial interface changes after BERT

  Conditions: "Any-phy" changes after running FPGA BERT for an interface if another interface on the same SPA having a lower "any-phy" value is deleted. Tracebacks are seen after provisioning new channel group.

  Workaround: Reload the SPA.

- 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.

- CSCsm40666

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

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

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

- 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.

- CSCsm41873

  Symptoms: Device crashes when VPN routing/forwarding (VRF) is unconfigured.

  Conditions: MCP Router crashes while unconfiguring **<ip vrf vrf name** with a script.

  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.

- CSCsm44147

  Symptoms: The standby WS-SUP720-3BXL failed to boot into SSO mode because of MCL check failure with the FPD configuration command: **upgrade fpd path sup-bootdisk:**

  Conditions: The problem happens when "sup-bootdisk:" is used as the FPD image package directory path argument in the **upgrade fpd path** *pkg-dir-path* configuration command for an active WS-SUP720-3BXL that supports "sup-bootdisk:" filesytem, but the same fiile system is not support by the standby WS-SUP720-3BXL.

  Workaround: For systems that have a mixture of old and new WS-SUP720-3BXL, please do not use "sup-bootdisk:" as the filesystem in the **upgrade fpd path** *pkg-dir-path* configuration command, instead use the "sup-bootflash:" filesystem as this filesystem exist on both old and new WS-SUP720-3BXL.

  Further Problem Description: The **show module** EXEC command can be used to identify the HW revision of the WS-SUP720-3BXL, if it does not have a version above 5.x then it won't have the support of the "sup-bootdisk:" filesystem.

- CSCsm44353

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

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

  Workaround: There is no workaround.

- CSCsm44620

  Symptoms: Multicast tunnel not coming up after RPM change. A misconfiguration with overlapping networks causes the join to be rejected. This can be seen on the PIM neighbor list.

  Conditions: There is a problem related to one of the hub card in rpm-xf.10 in forwarding PIM traffic from 2 PEs (rpm-xf.13 & rpm-xf.11). After RP migration from AVICI to CRS we found that tunnels from PE in slot 13 were not coming up. PE in slot 13 was in consistently in registering mode. PE was not coming out of registering mode which was preventing the tunnels from coming up. For PE to come out of registering mode S,G state should be built from new RP down to PE. At this stage the CRS (RP) showed that S,G tree was establish at the RP. S,G tree was OK all the way down from CRS to the last hop (P in slot 10) connecting to the slot 13 PE. The P router in slot 10, which is directly connected to PE, showed that S,G state was established and PE facing interface was in OIL. But there were couple of discrepancies on the P in slot 10. There were no flags set on this P for the mroute of PE. In addition, we found that PE was not receiving any PIM traffic from the P in slot 10. This led to suspicion that although the P showed the correct S,G and OIL but is still not able to forward traffic to the PE. And this could be the reason for PE to remain in registering mode hence preventing the tunnels from coming up.

Workaround: Remove the following configurations:

a. rpm-xfh10-z135 - shut & remove interface Switch1.4073

b. rpm-xfh09-z134 - shut & remove interface Switch1.4073

c. rpm-xfp11-l172 - remove interface Switch1.3172

d. rpm-xfp13-z074 - remove interface Switch1.4074

e. rpm-xfp04-l171 - remove interface Switch1.3171

- 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.

- CSCsm44905

  Symptoms: CPU Hog messages may be seen when QoS is configured on a number of subinterfaces

  Conditions: The symptom is observed in a scaled configuration with 4,000 subinterfaces having QoS applied, when a "match" statement is dynamically added or removed from the QoS class-map.

  Workaround: There is no workaround.

- 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.

- CSCsm45483

  Symptoms: Configuring local switching with auto-provisioned VC for an ATM interface configured with cell-packing through vc-class, results in the crash of a Cisco 7600 router.

  Conditions: This symptom is observed on an ATM interface on ATM SPA on a Cisco 7600 platform.

  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.

- CSCsm46170

  Symptoms: Upon the execution of the **test crash** command on the active supervisor in an HFS capable chassis, the new active fabric channel may go out of synchronization, the linecard shows up minor errors with the **show mod** command, the traffic stops passing through the linecard, and the following error message may be seen:

  ```
  %FABRIC_INTF_ASIC-5-FABRICSYNC_REQ: Fabric ASIC 0: Fabric sync requested after 3 sync
  errors
  ```

  Conditions: The symptoms are observed on an HFS-capable chassis and are triggered by the **test crash** command on the active supervisor. It is seen with both SIP200 and SIP400.

  Workaround: There is no workaround. The only way to come out of the problem state is with a line card reset using the **hw-module module** *slot* **reset** command.

- 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 linecard fails to come up displays the error messages.

  Workaround: Perform another OIR of the linecard.

- CSCsm47111

  Symptoms: Traceback is seen.

  Conditions: Occurs when certain memory checking is enabled.

  Impact: This is a fairly harmless issue. No impact.

  Workaround: Disable memory checking.

- 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

- CSCsm47944

  Symptoms: A Gigabit interface on an NSE150 flaps.

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

  Workaround: There is no workaround.

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

- CSCsm49143

  Symptoms: Extended ping parameters will not work for IPv6 source address if a VPN routing/forwarding (VRF) was specified on the initial command line.

  Conditions: The conditions to hit this bugs are: - Using the ping command with a VRF and a source address and, - specifying the source address via extended ping parameters rather that command line.

  Workaround: Use the command line to specify the source address.

- CSCsm49214

  Symptoms: ESM20G linecard 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.

- CSCsm50317

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

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

  Workaround: Remove the policy and reapply.

- CSCsm50741

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

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

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

- CSCsm51299

  Symptoms: CSCsl27236 did not catch all of the areas needed to be fixed due to code divergence.

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

  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:

  ```
  Jan 4 10:42:33.357 ROUTER: %IPRT-3-NDB_STATE_ERROR: NDB state error (BAD EVENT STATE)
  (0x00) 192.168.116.152/30, state 7, event 2->1, nh_type 1 flags 4 -Process= "RIP
  Router", ipl= 0, pid= 494
  ```

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

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

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

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

  clear ip route 192.168.116.152

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

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

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

- 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.

- CSCsm53196

  Symptoms: Crash occurs at "ip_route_delete_common".

  Conditions: Occurs under the following scenario:

  1)A multicast BGP route exists.

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

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

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

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

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

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

- 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 linecard. The traffic does not switch back to the primary TE- FRR tunnel on SIP-400 from backup tunnel on other linecard.

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

  Workaround: Toggle 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 linecard 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 linecard 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.

- CSCsm57474

  Symptoms: A VPDN-group configured with **ip mtu adjust** and with protocol PPTP, might result in crash of Cisco IOS 12.4T images. The MTU may not get adjusted on virtual-access on Cisco IOS 12.2SR images.

  Conditions: The symptoms are observed when **ip mtu adjust** is used to set virtual-access to adjust the MTU based on the outgoing L2TP tunnel IP interface. But this feature is not working for PPTP tunnels. Cisco IOS 12.4T images may experience a crash and Cisco IOS 12.2SR images may not adjust the MTU based on the outgoing tunnel interface.

  Workaround: Use the **ip pmtu** instead of **ip mtu adjust**.

  Further Problem Description: The problem is applicable to PPTP and not to L2TP.

- 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.

- CSCsm58240

  Symptoms: Traceback "%LSD-2-INVALID_VAR: app is not owner of label" may be seen while removing router Border Gateway Protocol (BGP) configuration.

  Conditions: Occurs in SSO mode when there are 1000s of routes in BGP table. If we try to remove router BGP configuration traceback is seen. There is no issue with forwarding of packets due to this.

  Workaround: Instead of removing entire **router bgp** config you could remove VPN routing/forwarding (VRF) address family in a step by step way to avoid this traceback.

- 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.

- CSCsm59499

  Symptoms: TOOBIG error messages 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 linecard 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.

- 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.

- 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- shut** 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** *number* under ATM interfaces

  Repeating Step 2 continuously will cause a crash.

  Workaround: There is no workaround.

- CSCsm61571

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

  Passing CLIs to the line card fail:

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

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

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

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

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

  Conditions: Occurs on a Cisco 7600 router with a XFP-10GZR-OC192 housed in a ES20, where the optical fiber has its RX level out of the specified range for the given XFP being used.

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

- CSCsm61726

  Symptoms: Adaptive clock stays in HOLDOVER state and does not get to an ACQUIRED state.

Conditions: The symptom is observed when using adaptive clock through an MLPPP interface. The same configuration with POS interfaces (instead of an MLPPP interface) will allow the adaptive clock get to an ACQUIRED state.

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.

- CSCsm62038

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

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

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

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

- CSCsm62179

  Symptoms: MPLS pseudowire ping for SVI Mode Ethernet over MPLS over GRE (EoMPLSoGRE) may fail.

  Conditions: The symptom is observed if EoMPLSoGRE is configured with SVI mode.

  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.

- CSCsm63632

  Symptoms: Watermark and XDR error messages indicating a failure to create IPC buffers are seen, such as:

  ```
  %XDR-6-XDRIPCPEER: XDR IPC error occurred for peer in slot 3/0 (3) due to inability to
  create an IPC buffer. %IPC-5-WATERMARK: 1123 messages pending in xmt for the port Slot
  3: FAST.control.RIL(2030000.11) from source seat 2160000
  ```

Conditions: The symptom is observed when the router is under stress by route flaps and linecard resets (DFC enabled) to create repeated downloads of the CEF tables to the line card(s). This creates large amounts of IPC traffic. Only releases prior to Cisco IOS Release 12.2(33)SRB3 are affected by this issue.

Workaround: There is no workaround, but XDR will recover from the situation gracefully without losing any messages.

Further Problem Description: It is not clear if other applications that fail to get IPC buffers during this period will recover gracefully or not.

- CSCsm64118

  Symptoms: The router may crash when the **no ip dhcp pool** *word* command is issued from the VTY.

  Conditions: This symptom is observed on a Cisco router when the **ip dhcp pool** *word* command is issued from the console and removed from VTY. Configuring dhcp class (class abcd) in the **ip dhcp pool** *word* mode, causes the router to crash.

  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.

- CSCsm68773

  Symptoms: LFI bundles will not come up.

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

  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.

- CSCsm69981

  Symptoms: ISG is not allocating the next free port in the cyclic order as expected.

  Conditions: The symptom is observed on PC clients using a web-portal. It is observed when the browser is shutdown and a new one started within 60 seconds and when the web-server timeout is set for 60 seconds.

  Workaround: Adjust the web-server TCP port allocation timers to match that of the ISG and PC clients.

  Further Problem Description: ISG allocates a free port in a port-bundle when a subscriber sends a TCP SYN packet. The port is freed after around 60 seconds. After this, if the same subscriber sends a TCP SYN packet (in order to establish a new session), ISG allocates the freed port and not the next free port in the cyclic order.

- 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.

- CSCsm70774

  Symptoms: The router crashes when a kron policy-list is modified from the console after that kron policy-list has been deleted by another user on a different vty.

  Conditions: This symptom can be observed on a Cisco router when the **kron policy-list** *word* is issued from the console and removed from the VTY. Using the command **cli** *abcd* in the console, while still in the **kron policy-list** *word* mode, causes the router to crash.

  Workaround. There is no workaround.

- CSCsm70913

  Symptoms: When a port channel interface (that is being used in the tunnel configuration) is deleted, then related configuration from the tunnel also should be removed.

  Conditions: When port channel interface (used in the tunnel configuration) is deleted.

  Workaround: There is no workaround.

  Further Problem Description: Following output shows the problem.

```
Router(config-if)#int loop 0
Router(config)#int tun 0
Router(config-if)#tun udlr receive-only loopback 0
Router(config-if)#no int loop 0
Router(config-if)#int loop 0
Router(config-if)#no tun udlr receive-only loopback 0
Router(config-if)#
*Apr 9 14:03:44.859: %TUN-4-UDLR_IDB_ERROR: UDLR Loopback0 - failed to disable
receive-only tunnel in udlr_tunnel_receive_only_remove (idbtype *udl_idb) we no longer
have udl_swsb on loop 0.
```

  All loop 0 config should be removed from tunnel when we delete the loopback interface.

  Loop 0 can be replaced by a port-channel interface.

- 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:

```
Dec 16 04:53:21: %DHCP_SNOOPING-3-DHCP_SNOOPING_INTERNAL_ERROR: DHCP Snooping internal
error, Unknown dhcp message type packet should be already handled so they should not
come here, they will be dropped. -Traceback= 405B938C 405B98D0 406125EC 41FE7E6C
41FE7D8C 41FE8940 41FE8A90
```

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

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

Workaround: Use RPR+ instead of SSO

- CSCsm72944

  Symptoms: Member links belonging to Multilink Frame Relay (MFR) bundles appear to be sending packets over freedm HIQ.

  Conditions: Display issue only. No functional impact.

  Workaround: There is no workaround.

- 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.

- CSCsm73220

  Symptoms: Archive created with many levels of subdirectories crashes the router.

  Conditions: Occurs under the following scenario:

  1. Create many levels of directories. 2. Perform archive "tar /create" on those directories.

  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
  ```

- CSCsm73592

  Symptoms: A reload may occur when an anything over MPLS (AToM) VC is torn down. Bug triggered initial crash of SIP-400 in slot 4 & ES20 in slot 3. Both cards had to be powered down and reset from the console to recover.

  Conditions: Occurs when AToM VC is setup and torn down later.

Workaround: There is no workaround.

Further Problem Description: The crash may occur when an event triggers access to a previously set up AToM VC. For example, the crash may occur when fast reroute (FRR) is configured on the tunnel interface and the primary interface is removed, such as in the following scenario:

```
pseudowire-class ER1_to_HR1_EoMPLS no preferred-path interface Tunnel501331
disable-fallback ! interface tunnel501331 shutdown ! no interface tunnel501331
```

- 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.

- CSCsm74143

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

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

  1) Remove the child policy from the parent class.

  2) Remove the service-policy from the subinterface.

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

- 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.

- CSCsm76792

  Symptoms: A standby supervisor power cycles over and over on boot up. The following errors are seen:

  ```
  May 14 19:21:09.188 EDT: %RF-SP-3-NOTIF_TMO: Notification timer Expired for RF Client:
  Cat6k Power(1318)
  ```

  Conditions: This has been experienced on a Catalyst 6500 with dual supervisors running Cisco IOS Release 12.2(33)SXH2a and Cisco IOS Release 12.2(33)SXH3.

  Workaround: There is no workaround.

- CSCsm76857

  Symptom: Adjacency turns incomplete when the same mac-address or different mac-address is reconfigured/configured under ATM interface. Packets go through but may be getting process switched.

Conditions:

1) This is observed on ATM interfaces

2) Observed when interfaces on the same box are looped back

3) IP address subnet configured on these interfaces are same but they are in different VRF.

Workaround:

There are 2 ways

1) Clear adjacency will make the adjacency complete. 2) Shut/No shut the interfaces.

- 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.

- CSCsm77558

  Symptoms: A "NODESTROYSUBBLOCK" error message is seen when the SWIDB is being reused and subblocks are still attached to the SWIDB.

  Conditions: The symptom is seen typically in thrashing situations or whenever sessions are being disrupted.

  Workaround: There is no workaround.

- CSCsm78047

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

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

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

- CSCsm78184

  Symptoms: The standby router may reload unexpectedly during synchronization, after a synchronization failure.

  Conditions: The symptom is observed during the MIB synchronization to standby.

  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.

- CSCsm78572

  Symptoms: With MLP, while sending UDP traffic and configuring RTP header compression, input errors occur in multilink. Also cRTP is not working. After configuring interleaving (with LFI) the traffic starts flowing without any input errors.

  Conditions: Occurs when the router is configured with MLP and cRTP

Workaround: Configure interleaving.

- 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.

- CSCsm80616

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

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

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

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

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

- CSCsm80847

  Symptoms: In SwEoMPLS scenario, a policy-map on the core facing ES20 interface matching on MPLS experimental topmost does not work.

  Conditions: The core facing ES20 interface should be first having a policy-map matching on input VLAN and then after removal of it and application of a policy-map matching on input VLAN would lead to this condition.

  Workaround: If the policy-map matching on MPLS experimental topmost bits was applied to the core facing ES20 interface without prior application of a policy-map matching on input vlan, this condition will not be hit.

- CSCsm82382

  Symptoms: A memory leak is seen on the Standby RP. If the memory leak is very high, CEF gets affected and finally gets disabled due to lack of memory. (It may take a few thousand such operations before the CEF gets disabled.)

  Conditions: The symptom is observed on a Cisco Catalyst 6500 series switch and the Cisco 7600 series router and while using 6348 line cards. The leak is seen in some port operations, such as port mode and port state changes.

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.

- CSCsm83812

  Symptoms: Router crashes various time while testing internal builds of Cisco IOS images. The following traceback is displayed:

  ```
  Router-2#test platform debugger address2sym 89A74B0 89A7628 A6FCC9C A6F2AF4 0x89A74B0
  ---> ipc_process_nonconf_sess_on_seat+F4 0x89A7628 --->
  ipc_service_nonconf_session_process+FC 0xA6FCC9C ---> ppc_process_dispatch+24
  0xA6F2AF4 ---> task_execute+28
  ```

  Conditions: The following steps were taken to reproduce the issue

  1) Toggle BGP (around 440,000) routes.

  2) Reset DFC and enable line card (3-4).

  Workaround: There is no workaround.

- CSCsm83961

  Symptoms: BFD for eBGP neighbors may not be enabled after an SSO switchover. Specifically, BFD sessions for eBGP neighbors that are up before an SSO switchover may not be present after an SSO switchover.

  Conditions: The symptom is observed with NSR peers on platforms that do not yet support BFD for SSO. When **neighbor** *ip- address* **ha-mode sso** and **neighbor** *ip-address* **fall-over bfd** are both configured for a neighbor, BFD is only enabled on the active RP. The fact that BFD has been enabled may be lost after issuing a forced switchover (even though the configuration is present and correct).

  Workaround: Configuring/re-configuring the **neighbor** *peer-ip-address* **fall-over bfd** command after the switchover will enable BFD for eBGP NSR peers. Rebooting the router will also have the same effect.

  Further Problem Description: Note that since BFD SSO is not yet supported, using both BFD and NSF for BGP simultaneously may cause BGP sessions to go down (and come back up) after an SSO switchover.

- 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.

- CSCsm87634

  Symptom: In the police flow command, the burst value may be different from the value that was inputted.

  Conditions: The symptom is observed when using the higher ranges of burst values, since the value is right-shifted before making a capability check.

  Workaround: There is no workaround if values closer to the upper limit are used. Additionally, if cir=128000, the issue will not occur as cir%8000 is 0 and hence the police factor is 0, so the right-shift does not take effect.

- 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.

- CSCsm87959

  Symptoms: An HSRP IPv6 address may become:: if the IP address of an interface is changed.

  Conditions: At least one HSRP IPv4 group should exist on the interface.

  Workaround: Delete the group completely from the configuration, and then reconfigure it.

  Once the problem occurs, the HSRP IPv6 group must be deleted and re-added.

- CSCsm88232

  Symptoms: Router crashes, resetting line cards and toggling 600,000 BGP routes.

  Conditions: Occurs when the system scale limit is exceeded, as there are more than 1200 unprocessed IPC messages. CPU stays at 100% for a long time.

  Workaround: There is no workaround.

- CSCsm88279

  Symptoms: Line card fails to boot when there are routes in the routing table.

  Conditions: This problem is seen very rarely with a large routing table.

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.

- CSCsm89526

  Symptoms: When a new class-map configuration is added to policy-map, packet (which belongs to another existing class) drop issue will be observed.

  Conditions: Occurs on a Cisco 7600 router with ES20 and running Cisco IOS Release 12.2(33)SRB.

  Workaround: There is no workaround.

- CSCsm89795

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

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

  Workaround: There is no workaround.

- 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.

- CSCsm92206

  Symptoms: A router may crash when a range of interfaces is set to default configurations.

  Conditions: The crash occurs when a range of interfaces is configured in a console connection to belong to a bridge group and when the same set of configurations is removed simultaneously from a vty connection.

  Workaround: Avoid simultaneous tasks (configuring/unconfiguring) through the console and vty.

- 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.

- CSCsm93068

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

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

  Workaround: There is no workaround.

- CSCsm93088

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

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

  Workaround: Delete and reconfigure again the bundle or reset the linecard.

- CSCsm93513

  Symptoms: Cannot configure queue-limit if more than one class has priority (with different priority levels) configured.

  Conditions: This is a new feature. Initially there was only one priority level supported, so only one queue was maintained. Queue-limit configurations were blocked if there were more than one priority class in the policy. Now that additional priority levels are supported, this configuration should be supported.

  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.

- 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.

- CSCsm95129

  Symptoms: The **no ip next-hop-self eigrp** command does not work after mutual redistribution with BGP (either iBGP or eBGP).

  Conditions: This has been observed on any platform. The combination RIP/EIGRP or OSPF/EIGRP works instead.

  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.

- CSCsm95456

  Symptoms: Duplicate L3 packets may occur on a Cisco Catalyst 6500 switch.

  Conditions: The symptom is observed on a Cisco Catalyst 6500 switch, configured with an L2 Distributed Ether Channel (DEC) and with WS-X6708 blade (s) installed. This issue is due to the mix of 3A/3B and 3C PFC/DFC (and will not occur in a pure 3A+3B or 3C PFC/DFC system). It occurs when: 1. There is a mix of 3C and 3B (or 3A). 2. There is at least one L2 DEC in the system.

  Workaround: Do not use an L2 DEC.

- CSCsm96355

  Symptoms: A Cisco 7600 running a Cisco IOS Release 12.2SR image might experience a small amount of packet loss (about 10-20 ms) during TE-FRR reoptimization. This happens only for EVC (Ethernet Virtual Circuit) or scalable Ethernet Over MPLS (EoMPLS) configurations with large number of traffic engineering (TE) tunnels.

  Conditions: This issue happens only for traffic going over EVC or scalable EoM VCs when the box has scaled configuration, such as a large number of TE tunnels.

  Workaround: There is no workaround.

- 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.

- CSCsm96785

  Symptoms: You may observe a problem which the OSPF neighbor is down after switch-over in spite of using OSPF Non-Stop Forwarding (NSF).

  Conditions: This occurs with the following conditions: - "nsf cisco" is only affected. If "nsf ietf", this problem does not occur. - You may observe this problem if the OSPF interface is "point-to-multipoint non-broadcast" or "point-to-multipoint". If the interface is "broadcast", this problem does not occur. - When this problem occurs after switch-over, DBD packet may not be exchanged between two neighbors. And the neighbor is down in spite of NSF.

  Workaround: Change the OSPF config to "nsf ietf" and change the OSPF interface to "broadcast".

- CSCsm96842

  Symptoms: The command **hold-queue** *length* **in** cannot be configured for port-channel interface.

  Conditions: The symptom is observed with a Cisco 7600 series router after upgrading to Cisco IOS Release 12.2(33)SRC.

  Workaround: There is no workaround.

  Further Problem Description: Queueing is not supported for port-channel with a Cisco 7600 series router. The hold-queue is a legacy queueing command and is not supported.

- CSCsm97297

  Symptoms: Output direction ACL does not work.

  Conditions: Occurs when **ip cef accounting** is enabled on a MPLS enabled router doing tag disposition. If packets coming in are tagged, and they are going out of the router as untagged, the output IP ACL may not work.

  Workaround: Reconfigure the static route or clear the route.

- 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 ENGINEERING WEEKLY BUILD (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 currently 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.

- CSCsm99079

  Symptoms: The kron process may generate the following syslog and cause the device to reload:

  ```
  Dec 30 23:47:31.920: %SYS-3-CPUHOG: Task is running for (2004)msecs, more than
  (2000)msecs (1/0),process = Kron Process. -Traceback= 0x42725288 0x42725778 0x42724AC0
  0x41E0D72C 0x41E0E0BC 0x41E0E3FC
  ```

  Conditions: The symptom is observed when the command **kron** is configured with the *at* parameter.

  Workaround: Try redesigning the **kron** command to use the *in* parameter.

- CSCsm99651

  Symptoms: Link down notification is slow on ES-20.

  Conditions: Occurs on 10GE ports of ES-20 linecard, 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.

- CSCso00104

  Symptoms: Modifying the aggregation-type prefix-length under Optimized Edge Routing (OER)/learning, along with the ACL used by oer-map for traffic matching can lead to router crash

  Conditions: The router crash was observed when aggregation-type prefix-length and the ACL used by OER-MAP was changed. The aggregation-type prefix-length can be configured as: ! oer master learn aggregation-type prefix-length 16 !

  The OER-MAP can be configured as follows: (in this case, oer-map is used to set monitor mode to active for the traffic matching the ACL) ! oer-map BRANCH 10 match traffic-class access-list OerMapAclHttp set mode route control set mode monitor active set unreachable threshold 10 set active-probe echo 10.1.6.254 set probe frequency 10

  Workaround: After making the configuration changes, if the configuration is saved right away, and then the router is reloaded, the crash was not observed. This can be used as a workaround for this crash.

- CSCso00793

  Symptoms: Enhanced-Flexwan crashes with cache error with MEM-CC-WAN-512M=, version "VI4DP647228EBK-MD" installed.

Example of Symptom:

```
Cache error detected! CP0_CAUSE (reg 13/0): 0x00004000 CPO_ECC (reg 26/0): 0x40000000
Data cache error CPO_BUSERRDPA (reg 26/1): 0xFFDFFFE0 CPO_CACHERI (reg 27/0):
0x200011C0 Tag address parity error Instruct cache index 0x0000008E CPO_CACHERD (reg
27/1): 0x840000A0 Multiple data cache errors External cache error Data cache index
0x00000005 CPO_CCHEDPA (reg 27/3): 0x09271600
Interrupt exception, CPU signal 20, PC = 0xA0000100
-Traceback= 40723DA8 406AF1B0 406B5BC8 406BAAF8 406BC200 406B4788 4072AA0C 4011D870
4012D204
```

Conditions: This issue is seen under certain conditions, which are not fixed. No specific trigger.

Workaround: There is no workaround.

- CSCso01440

  Symptoms: PE1 2/2/1 <--------> 4/0/1CE1

  Connect SPA-4XCT3/DS0 SPA back to back, configure loopback network at CE1, and then run bert on 4 T1 channels in PE1. After this, bert will not stop even though the time interval elapsed.

  Conditions: All the interfaces should be up and running.

  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.

- 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.

- CSCso03783

  Symptoms: Router stuck in UNKNOWN-MODE and not accepting any commands.

  Conditions: Occurs after configuring xconnect VC through interface range mode

  Workaround: Power cycle the router.

- 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.

- CSCso04657

  Symptoms: SSLVPN service stops accepting any new SSLVPN connections.

Conditions: A device configured for SSLVPN may stop accepting any new SSLVPN connections, due to a vulnerability in the processing of new TCP connections for SSLVPN services. If “debug ip tcp transactions” is enabled and this vulnerability is triggered, debug messages with connection queue limit reached will be observed. This vulnerability is documented in two separate Cisco bug IDs, both of which are required for a full fix: CSCso04657 and CSCsg00102.

- CSCso04932

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

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

  Workaround: There is no workaround.

- CSCso05177

  Symptoms: User-defined class and non-shape based queuing policy can be attached to a tunnel interface. This should not be allowed.

  Conditions: Occurs in internal builds of Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- CSCso06346

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

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

  Workaround: There is no workaround.

- CSCso06402

  Symptoms: Unconfiguring the router may force the router to crash.

  Conditions: The symptom is observed when unconfiguring the router and where the route-map is configured with DF bit set/unset.

  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.

- CSCso07411

  Symptoms: In a router having redundant RP and configured for stateful switchover (SSO), traffic engineering (TE) tunnels and Open Shortest Path First (OSPF) as IGP configured, the standby RP may continue rebooting after a SSO switchover and the following config-sync error will be seen in the console log:

  ```
  Mar 5 13:14:19.749 PST: Config Sync: Bulk-sync failure due to Servicing
  Incompatibility. Please check full list of mismatched commands via: show redundancy
  config-sync failures mcl
  Mar 5 13:14:19.749 PST: Config Sync: Starting lines from MCL file: interface
  Tunnel3000 ! <submode> "interface" - ip ospf interface-retry 0 ! </submode>
  "interface"
  ```

Conditions: The symptom will only happen in a mis-configuration where the TE tunnel interface does not have an IP address configured.

Workaround: Tunnel using OSPF as IGP is required to configure tunnel IP address in order to forward IP traffic. To fix this mis-configuration, use the loopback address for TE tunnel interface IP address, such as **ip unnumbered loopback 0** for tunnel address.

- 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)

  ```
  Mar 2 22:17:19.796: RADIUS: Calling-Station-Id [31] 15 "0|4|6aac.fc82" Mar 2
  22:17:19.796: RADIUS: NAS-Port-Type [61] 6 Ethernet [15] Mar 2 22:17:19.796: RADIUS:
  Vendor, Cisco [26] 32 Mar 2 22:17:19.796: RADIUS: Cisco AVpair [1] 26 "circuit-id-
  tag=0|0|9|2|6" Mar 2 22:17:19.796: RADIUS: Vendor, Cisco [26] 35 Mar 2 22:17:19.796:
  RADIUS: Cisco AVpair [1] 29 "remote-id- tag=0|4|6aac.fc82" Mar 2 22:17:19.796: RADIUS:
  NAS-Port [5] 6 16777329 Mar 2 22:17:19.796: 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.

- CSCso09607

  Symptoms: All or some of the following symptoms may be experienced: 1. Crash could occur during GTPLB sticky timer expiration. 2. Crash could occur if **show ip slb sticky gtp imsi** command is issued. 3. "%SLB-4-UNEXPECTED: Unexpected error: real num_clients counter already 0" message might be displayed. 4. Unexpected timer expiration for the same sticky object could occur. This could be realized only with **debug ip slb sticky gtp imsi**. The frequency of expiration might increase periodically.

  Conditions: The symptoms are observed under all of the following conditions: - GTPLB sticky and non-zero sticky idle timer should be configured under vserver. - Query should be configured under vserver. - At least one NSAPI's pdp session context should have been deleted in GGSN which is not known to GTPLB when GGSN receives the pdp status query for all NSAPIs from GTPLB. - On sticky timer expiration, the response for GTPLB query should contain status for fewer number of NSAPIs than GTPLB has. Sticky object with the NSAPI should have been deleted after n number of retries and the deletion should have occurred at least twice.

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.

- 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.

- 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.

- CSCso10824

  Symptoms: Standby RP continually rebooting with a client progression failure.

  Conditions: Standby RP is booting in an stateful switchover (SSO) configuration. A Client Progression failure is reported, and standby repeatedly reboots.

  Workaround: Change the mode to RPR.

- 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.

- CSCso12305

  Symptoms: The IPv6 Cisco Express Forwarding (CEF) table may be missing prefixes which are present in the IPv6 RIB.

  Conditions: Occurs when CEF is disabled and re-enabled.

  Workaround: Enter the **clear ipv6 route ***.

- 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.

- 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.

- CSCso15725

  Symptoms: Module's configuration not synchronized to standby supervisor if module resets while standby is booting up.

  Conditions: This bug may be seen if linecard or SPA were to reset before standby reaches standby hot terminal state.

  Workaround: Use **redundancy reload peer** to reset standby supervisor. On its next boot, configuration is synchronized to standby.

- CSCso15740

  Symptoms: The "set metric" clause in the continue route-map sequence is not setting metric correctly in some particular conditions. This is also applicable in case where the nexthop setting is done via route-map with a continue clause.

  Conditions: The symptom is observed on a Cisco 12000 series router that is running Cisco IOS Release 12.0(32)SY4. This is platform independent. This symptom occurs if the route-map has a continue clause and the match condition does not allow the continue clause to be executed. The following route-map sequence which has to be executed will not execute properly if the metric or nexthop of the prefix are to be modified via the route-map.

  Workaround: Avoid using "continue" in a route-map and modifying metric or nexthop via the following route-map sequence.

- CSCso17473

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

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

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

  Frequency: Easily reproducible.

  Trigger: Switchover.

  Impact: The standby reloads continuously.

  Workaround: Upgrade the Cisco IOS software.

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

- CSCso17733

  Symptoms: Stop record not generated when PPPoA session goes down to make Multilink PPPoA bundle come up with virtual-access interface (both normal and sub-interface).

Conditions: Issue is seen only when PPPoA session goes down to make Multilink bundle UP, over normal PPPoA session. Here normal PPPoA session goes down and brings up multilink PPPoA session with virtual-access (both normal and sub) interface, as we configure **ppp multilink** on virtual-template.

Workaround: There is no workaround.

- CSCso18630

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

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

  Workaround: There is no workaround.

- 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.

- 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.

- CSCso25823

  Symptoms: Router causes neighbor router to crash.

  Conditions: Error message are seen when "mpls ip" is enabled on the interface, but causes the neighbor router to crashes upon issuing the command.

  Workaround: There is no workaround.

- 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.

- 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.

- CSCso27236

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

  ```
  Before restart Start Date: 1 Jan 2008 10:00:00 End Date : 1 Jan 2011 10:00:00 Renew
  Date : 1 Jan 2008 09:58:00
  After restart Start Date: 1 Jan 2008 10:00:00 End Date : 1 Jan 2011 10:00:00 Renew
  Date : 1 Jan 1970 08:00:00
  ```

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

  Workaround: There is no workaround.

- CSCso28309

  Symptoms: Ping fails from reflector during internal testing.

Conditions: The goal of the test is to verify the successful termination of PPP/PPPoE over ATM sessions on router's ATM interface using auto sensing. It is performed with auth_pap, process switch, and keepalive disabled. This has a functional impact as the virtual access entry is not getting added to the routing table after doing clear ip route.

Workaround: There is no workaround.

- CSCso30598

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

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

  Workaround: There is no workaround.

- CSCso30669

  Symptoms: The standby RP continuously reloads after showing the following error message: HA-6-INT_SSO_UNAWARE

  Conditions: The symptoms are observed only when a Virtual Router Redundancy Protocol (VRRP) group is configured on one of the RP native GE-interfaces on a Cisco 7304 router (which does not currently support SSO).

  Workaround: VRRP can be configured on the Gigabit Ethernet Shared Port Adapter (SPA) interfaces on this platform, which are fully SSO-aware.

- CSCso30819

  Symptoms: Occasionally upstream traffic may be dropped when a private VLAN is configured, and after an OIR or the **shutdown** followed by the **no shutdown** commands are used.

  Conditions: The symptom is observed after sending untagged upstream traffic using the secondary/isolated VLAN from the promiscuous port. After using the **shutdown** and **no shutdown** command sequence (or an OIR), traffic may get dropped due to CBL logic being in the improper state.

  Workaround: Reload the system.

- 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.

- CSCso33454

  Symptoms:

  PART 1) In a PE CE setup when 500 BGP VRF sessions are configured on a Cisco 10000 router, the PE PRE goes out of memory. PART 2) In a PE CE setup when 600 BGP VRF sessions are configured on a Cisco 10000 router, the PE PRE goes out of memory and crashes.

  Conditions: The symptoms are seen under the following conditions:

  PART 1) The number of routes is 500*500 /31 routes and 500*220 /24 routes. PART 2) The number of routes is 600*600 /31 routes.

  Workaround: There is no workaround.

- CSCso33848

  Symptoms: PPP call may fail with stack group configured.

  Conditions: Failure will happen only when call initiated to stack group member

  Workaround: Initiate PPP call directly to stack group master.

- 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.

- CSCso37750

  Symptoms: In Cisco-data-collection MIB, when SNMP bulk transfer is configured and unconfigured the switch crashes. The following Buffer Overflow message is displayed:

  ```
  Mar 19 22:59:05.272 PST: %SNMP_BULKSTAT-4-BUFFER_OVERFLOW: Buffer size too small to
  accommodate data for one collection interval for myTransfer
  ```

  Conditions: Occurs when SNMP bulk transfer is configured and unconfigured.

  Workaround: There is no workaround.

- 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.

- CSCso38472

  Symptoms: The **random-detect precedence** command is not accepted under class in a Cisco 10000 policy-map configuration.

  Conditions: This symptom is observed in the following Cisco IOS Release 12.2 (33)SB images:

  c10k3-p11-mz.122-32.9.24.SB c10k3-p11-mz.122-32.9.19.SB c10k3-p11-mz.122-32.8.98.SBK05

  Workaround: There is no workaround.

- CSCso39171

  Symptoms: When issuing the **show mac-address-table** command for an interface with REP enabled on a Cisco 7609, the Telnet session hangs and the system becomes unresponsive for long periods of time until CPU drops.

  Conditions: Occurred on a router running Cisco IOS Release 12.2(33)SRC1 and when REP is configured.

  Workaround: Remove REP configuration.

- CSCso39217

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

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

  Workaround: There is no workaround.

- 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.

- CSCso39597

  Symptoms: The redundant RP in a dual-RP router may crash in certain cases when BGP is unconfigured and then an SSO is performed.

  Conditions: The symptom is observed on a redundant RP in a dual-RP router that is running Cisco IOS Release 12.2(33)XN with BGP VPNv4 configuration. It is observed when BGP is unconfigured first and then an SSO is performed.

  Workaround: Avoid unconfiguring BGP prior to an SSO.

  Further Problem Description: The problem is platform independent. After the reset, the redundant RP is able to function normally.

- CSCso40442

  Symptoms: When a router is configured for a redundancy mode other than SSO, BGP sessions may remain in an idle state after an RP switchover.

  Conditions: The symptom is observed after an RP switchover when the redundancy mode configured on the router is not SSO (for example, RPR and RPR+ modes exhibit this problem).

  Workaround: Reload the router.

  Further Problem Description: Until the router is reloaded, all incoming BGP open messages will be ignored and the router experiencing the problem will not initiate any outbound opens.

- CSCso40678

  Symptoms: Multilink PPP interface may cease passing traffic after one of the MLP group's member links receives an AIS from the TDM network.

  Conditions: Problem occurs on a Cisco 7600/SUP-720/OSM/CHOC12/T1-S1 running the c7600s72033-adventerprisek9-mz.122-33.SRB2 image.

  Workaround: Perform a shut/no shut of the multilink interface.

- CSCso41513

  Symptoms: When using the **ip helper-address** command to forward directed broadcast, an incomplete ARP entry will be created for the helper-address configured even if it is not a directly connected subnet. This may break BOOTP forwarding to the DHCP server.

  Conditions: The symptoms are observed in Cisco IOS Release 12.4(19) only. Cisco IOS Release 12.4(18) does not have this issue.

  Workaround: Configure proxy-arp on the next hop device on the path to the DHCP server.

  Alternate Workaround: Configure static ARP on the router for the helper-address pointing toward the next hop.

- CSCso41824

  Symptoms: A router crashes with an unexpected exception to CPU vector 300.

  Conditions: This symptom is observed when you configure MPLS trunks on an 4xT3E3 SPA with FR IETF encapsulation.

  Workaround: There is no workaround.

- CSCso42792

  Symptoms: A router does not boot with the secured image after securing the image an the disk.

  Conditions: This happens on a Cisco router loaded with Cisco IOS Release 12.4(19.9)PI8.

  Workaround: There is no workaround.

- 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.

- CSCso46427

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

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

  Workaround: There is no workaround.

- 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.

- CSCso48665

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

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

  Workaround: There is no workaround.

- CSCso49388

  Symptoms: Router crashes on attaching the policy which contains "queue-limit" configuration in the input direction of any interface.

  Conditions: Occurs on Cisco 7200 routers with NPEG1 processor and Cisco 7301 routers.

  Workaround: There is no workaround.

- CSCso49598

  Symptoms: Standby reloads continuously when "MAXINT" is used with "int ran" to create logical interfaces using.

  Conditions: Occurs in SSO mode.

  Workaround: Avoid giving MAXINT as range.

  Further Problem Description: At a stretch, only 1000 logical interfaces could be created through interface range. Due to some wrap-around problem, it was not showing error when MAXINT was given as option and starts creating these many interfaces which are much beyond the MAXINTERFACES supported by any existing platform. It will lead to MEMORY getting exhausted and different after effects as standby reload.

- 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.

- CSCso50363

  Symptoms: When AAA authentication is from RADIUS and RADIUS debugs are enabled, the password (except for last two characters) for the users trying to login to the box appears in debug messages.

  Conditions: Occurs under the following scenario:

  1) Configure RADIUS server.

  2) Configure AAA authentication for login with RADIUS.

  3) Enable RADIUS debugs.

4) Try to telnet to the router.

Workaround: There is no workaround.

- CSCso50383

  Symptoms: In a Cisco 7600 ring topology with TE-FRR configuration, traffic might get software switched if the packet comes in on a interface and goes out of the same interface.

  Conditions: This can happen in a 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.

- CSCso50484

  Symptoms: An RSVP GR instance may not be created on a sub-interface. Additionally, the interval of GR instance may change to 200 when the backup tunnel on the interface is flapped.

  Conditions: The symptoms are observed after the **shutdown** and **no shutdown** commands are executed on the main interface where the sub-interfaces are created. The other trigger is when the backup tunnel on the interface is flapped.

  Workaround: Unconfigure and reconfigure global RSVP GR.

- CSCso50587

  Symptoms: FRR Protection is failing after using the **no shutdown backup tunnel** command.

  Conditions: The symptom is observed after adding for the first time an FRR flag over a TE tunnel using the command **tunnel mpls traffic-eng fast re-route**.

  Workaround: Use the **shutdown** command followed by the **no shutdown** command on the Primary Tunnel.

- CSCso50602

  Symptoms: Router reloads after the **show ip bgp ipv4 mdt vrf** command is entered.

  Conditions: Occurred on a Cisco 7600 router running Cisco IOS Release 12.2(33)SRB2. Occurs when the **show ip bgp ipv4 mdt vrf** command entered with the *ip address* option, such as **show ip bgp ipv4 mdt vrf abc123** *x.x.x.x*.

  Workaround: The reload can be avoided by not using the IP address option with the 'show ip bgp ipv4 mdt vrf' command. None of the other options available for this command will trigger a reload

- 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.

- CSCso51519

  Symptoms: Paths with same next-hop may be marked as being multipath.

Conditions: The symptom is observed when multipath is configured and when using RRs in the environment.

Workaround: There is no workaround.

- CSCso51637

  Symptoms: Router crashes.

  Conditions: Router may crash in some cases after removing interface Auto-template and unconfiguring auto-mesh with large number of active mesh auto-tunnels. Currently, this crash has only been observed occasionally with internal scale test scripts and has not occurred with manual configuration.

  Workaround: Wait till all auto-tunnels are down after unconfiguring auto-tunnel mesh globally, and before removing interface Auto-template

- CSCso51661

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

  router ospf 1 shutdown

  Conditions:

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

- CSCso52344

  Symptoms: On an RP, the **show ip cef** command displays the nexthop as drop for the 224.0.0.0/4 prefix, but on the linecard the nexthop is displayed as multicast.

  Conditions: This issue occurs when **ip multicast-routing** is not configured and when the command **show ip cef** is issued on the RP and linecard.

  Workaround: There is no workaround.

  Further Problem Description: This is a cosmetic issue.

- CSCso52598

  Symptoms: The router may crash after the **no interface ethernet** *0/0.1* command is entered.

  Conditions: It could happen on a router with more than 4000 dynamic ARP entries.

  Workaround: Do not execute **no interface ethernet** *0/0.1*.

- CSCso52837

  Symptoms: While executing "copy run disk0:test" the following error is received:

  ```
  %Error parsing filename (No such device)
  ```

  Conditions: The symptom is observed on a router that is running Cisco IOS Release 12.4T.

  Workaround: Use a "/", as in "copy run disk0:/test".

- CSCso53306

  Symptoms: A Cisco IOS device may crash with a data bus error exception and stack trace PC = 0xA0000100

  Conditions: Device is running normal production traffic. Presence of malformed punted RP packets in this network caused the issue.

  Workaround: There is no workaround.

- CSCso53332

  Symptoms: A Cisco 7600 series router acting as an ISG may run into memory issues.

Conditions: The symptom is observed when a DHCP-initiated session is brought up on a default (null) VRF causing the standby router to run into memory corruption issues. This can lead to malloc failure tracebacks or, in some instances, crash the standby router.

Workaround: There is no workaround.

- CSCso53377

  Symptoms: With large number of label switched paths (LSP), the SSO recovery process may take longer than expected. Therefore sometimes not all traffic engineering (TE) LSPs can recover after SSO switchover.

  Conditions: Occurs on when there is a large number of LSPs.

  Workaround: There is no workaround.

- 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.

- CSCso53557

  Symptoms: A Flexwan 2 linecard may crash after removing and re-applying the WRED.

  Conditions: The symptom is observed when a policy-map is applied under a PVC FR in main interface then a subinterface is configured, and the PVC FR and the map- class is moved to the sub-interface. Then the sub-interface is deleted and the policy-map is applied to the main interface directly. Following this, the WRED is unconfigured and re-configured in class-default.

  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.

- 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.

- CSCso55081

  Symptoms: Synchronization from the Active RP to the Standby RP may not occur. It may halt during PPP negotiation and stop at AAA sync.

  Conditions: The symptoms are observed during synchronization and where the CoA feature is available for the image and platform.

  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.

- CSCso55799

  Symptoms: The **random-detect precedence** command is not accepted under class in a Cisco 10000 policy-map configuration.

  Conditions: This symptom is observed in the following Cisco IOS Release 12.2 (33)SB images:

  c10k3-p11-mz.122-32.9.24.SB c10k3-p11-mz.122-32.9.19.SB c10k3-p11-mz.122-32.8.98.SBK05

  Workaround: Use the **random-detect aggregate** command, instead of the **random-detect** command before the **random-detect precedence** command.

- CSCso55933

  Symptoms: A SIP-400 may crash during RP switchover with scale configuration and heavy load.

  Conditions: The symptom is observed with a Cisco 7600 series router with HA scale configuration and with 28K VC and 500 VPLS.

  Workaround: There is no workaround. The LC will recover after a reload.

  Further Problem Description: This crash shows up rarely during RP switchover. LC will self-recover after a reload.

- CSCso56101

  Symptoms: Some CFM remote MEPs may not appear as up when connected by a SIP-400 linecard.

  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.

- CSCso56413

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

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

Workaround: There is no workaround

- CSCso57001

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

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

  Workaround: There is no workaround.

- 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.

- CSCso57886

  Symptoms: A Cisco IOS device may crash with a data bus error exception and stack trace PC = 0xA0000100

  Conditions: Device is running normal production traffic. Presence of malformed punted RP packets in this network caused the issue.

  Workaround: There is no workaround.

- CSCso59251

  Symptoms: An interface on ESM20G goes down.

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

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

- CSCso59390

  Symptoms: After second switchover, a Cisco 7600 only forwards downstream traffic at 100 pps rate to the ISG IP client.

  Conditions: The 7600 router has the sip400 linecard on the access side and a WS-X6704-10GE card on the core side. IP data traffic were sending bidirectionally at rate 500 pps with 128 bytes packet size. After the first SSO, traffic were not impacted and both directions were able to forward at 500 pps, but after the second SSO downstream traffic rate dropped to 100 pps.

  500 pps --------> sip400- 7613- 6704----------> 500 pps 100 pps <-------- sip400- 7613- 6704-<---------- 500 pps

ISG session profile has:

* 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

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.

- CSCso59974

  Symptoms: BGP seesion goes idle.

  Conditions: Occurs following a stateful switchover (SSO).

  Workaround: There is no workaround.

- CSCso61282

  Symptoms: Multicast traffic from a VRF may be dropped after encapsulation.

  Conditions: The symptom is observed when a Bidirectional PIM (bidir-PIM) is used in the core network and VRF traffic is forwarded through a data MDT. In this condition, SSO switchover may trigger a packet drop issue.

  Workaround: Use the **clear ip mroute** *group* command.

- CSCso62193

  Symptoms: The standby router may reset unexpectedly.

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

Workaround: There is no workaround.

- CSCso62526

  Symptoms: Standby supervisor reloads after the interface configuration command **no flow-sampler <name>** is used to remove flow sampler map.

  Conditions: Occurs on a Cisco 7606s with two RSP720-3C-GE configured for normal use with sampled NetFlow configured. To cause the issue, a sampler must be explicitly detached.

  Workaround: There is no obvious workaround to the issue. To avoid the issue, avoid detaching the sampled NetFlow.

- CSCso63263

  Symptoms: The RP will start showing IPC-5-WATERMARK: 988 messages pending in xmt for the port messages on the screen. The number of messages will change.

  Conditions: The router has 275,000 i-BGP routes injected into the router. Among these routes, 100,000 are flapped continuously for one to one and half days. They are flapped every 10 sec. The problem needs at least a days worth of time of continuous flapping.

  Workaround: Stop the route flap. Although the messages will keep coming, there is no impact on functionality. And they are bogus since they are originated from wrong count.

- CSCso63807

  Symptoms: Packet loss when pinging an IP Address in a VPN routing/forwarding (VRF).

  Conditions: This problem is seen on a Cisco 7600 after the VRF configuration on a port is rapidly changed, such as the following example:

  interface gi3.1.88 ip vrf forwarding aaaa ip vrf forwarding bbbb

  Workaround: Delete the VRF with **no ip vrf forwarding aaaa** before changing the VRF under the interface.

  Further Problem Description: The VLAN RAM, which stores the VRF ID, is programmed wrong when this issue is seen. This causes packet loss or packets to be punted to the RP to resolve the conflict

- CSCso64050

  Symptoms: Policy-map outputs are not seen in standby router. The policy is attached to the VC in the standby, but no output is seen.

  Conditions: The symptom is observed when an ATM PVC is created and a service policy is attached to the PVC.

  Workaround: There is no workaround.

- CSCso64104

  Symptoms: A router may crash after applying the configurations related to PA- MC-2T3-EC immediately after the router reloads.

  Conditions: The symptom is observed on Cisco 7200 series and a 7301 router.

  Workaround: Do not configure PA-MC-2T3-EC immediately after the router reloads.

- CSCso64422

  Symptoms: Processing of certain external routes with EIGRP is incorrect.

Conditions: The external information, such as originating router id, originating protocol, is 0.

Workaround: There is no workaround.

- CSCso64607

  Symptoms: A router may crash when the **no ip vrf** command is issued.

  Conditions: The symptom occurs when VRF was previously configured on a tunnel interface that has subsequently been removed.

  Workaround: Possibly unconfigure **ip vrf** before unconfiguring the tunnel interface.

- CSCso65193

  Symptoms: The memory occupied by the IP SLA Event Processor may gradually increase.

  Conditions: The issue occurs when IP SLA jitter operation is configured on the router without source port specification.

  Workaround: There is no workaround.

  Further Problem Description: With 1000 IP SLAs configured (200 each of following types: path-echo, path-jitter, icmp-echo, udp-jitter and udp-echo, each with a unique destination), the memory allocated for "IP SLAs Event Pr" increases and the level of available processor memory goes down. This issue will have a performance impact.

- CSCso66516

  Symptoms: Memory allocated at function "_fib_table_test_cef_table_route_list" function is leaked.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS 12.2(33.02.19)SBK06 and that is configured for CEF-MTR

  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** *number* under ATM interfaces.

  Repeating Step 2 continuously will cause a crash.

  Workaround: There is no workaround.

- CSCso67141

  Symptoms: When a Border Gateway Protocol (BGP) peer is brought down, some of the routes that were learned may not be removed. If around 200,000 routes are advertised from a neighbor and the BGP process on the neighbor is then stopped, all routes will be removed the first time. On the second time, however, around 20,000-80,000 routes may remain.

  Conditions: The symptom occurs when the BGP process on the neighbor (that has advertised 200,000 routes or more) is brought down.

  Workaround: There is no workaround.

- CSCso67195

  Symptoms: Router may crash due to memory corruption:

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

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

  ip pim sparse-dense-mode

  access-list 98 deny any log

  Workaround: Remove access-list logging.

- CSCso67500

  Symptoms: Multicast traffic from the VRF network may be dropped after encapsulation.

  Conditions: The symptom is observed when a Bidirectional PIM (Bidir PIM) is used in the VRF network and when Gigabit port(s) on the active supervisor are in use. An SSO switchover can trigger a packet drop issue.

  Workaround: Reconfigure MDT using the **no mdt default** command followed by the **mdt default** *group- address* command.

- CSCso67850

  Symptoms: When pasting (as in cut-and-pase) a set of IPv6 configuration commands for a router network interface to the router console, the router may crash.

  Conditions: Issue may occur during router configuration.

  Workaround: There is no workaround.

- CSCso68344

  Symptoms: The command **no service dhcp** to stop DHCP server/relay from the router may cause a crash.

  Conditions: The symptom is observed when router is receiving requests from DHCP clients at high rate and duplicate-address detection ping is active.

  Workaround: There is no workaround.

- CSCso70986

  Symptoms: When traffic engineering (TE) preferred path is removed, then all the XCs using that pw-class are unprovisioned.

  Conditions: Occurs when xconnect anything over MPLS (AToM) configured with TE tunnel preferred path.

  Workaround: There is no workaround.

- CSCso71350

  Symptoms: The standby may reload when upgrading the software from Cisco IOS Release 12.2(31)SB to Release 12.2(33)SB. After issuing the **issu loadversion** command, when the standby tries to boot up with Cisco IOS Release 12.2(33)SB, it fails and may crash at **config sync** and may continually reboot.

Conditions: The symptoms occur when synchronizing a virtual template/virtual access interface configuration from the active to the standby.

Workaround: There is no workaround if virtual access interfaces are required.

- CSCso72167

  Symptoms: The ISSU AAA client negotiation says the session is COMPATIBLE with the images, even though the standby is loaded with an image that does not support that client.

  Conditions: The symptoms are observed when there is a stale ISSU AAA client on the ACTIVE, which does not clear the session once the standby goes down.

  Workaround: There is no workaround

- CSCso72541

  Symptoms: The **show ipv6 mfib active** yields the following error message:

  ```
  "%MFIB_STATS-DFCx-x-MFIB_STATS_LC_FAILED_GET_COUNTERS: Linecard failed in getting
  counters due to null table"
  ```

  Conditions: The error message is seen when we have active IPv6 multicast sources sending packets at a rate greater than 4 kbps.

  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.

- CSCso73533

  Symptoms: Traceback is seen after unconfiguring the tunnel interface.

  Conditions: The symptom is seen when using Ipv4 multicast PIM tunnels where the route to the Rendez-Vous Point (RP) is via another tunnel interface. If this tunnel interface was unconfigured, then there is a race condition between: 1. learning about the new route to the RP via another interface; and 2. periodic update of the PIM tunnel adjacency. If the latter occurs first the traceback is seen

  Workaround: There is no workaround.

- CSCso74028

  Symptoms: The local PE is sending graft messages even after receiving data from the remote PE on an MVPN network.

  Conditions: This symptom is observed when the graft-ack messages are lost in transit (could be due to misconfiguration/ACL, etc.).

  Workaround: Fix the misconfiguration so that graft-ack messages are forwarded as expected.

- 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

- 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.

- 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.

- CSCso74843

  Symptoms: The standby may hang during boot, and the master enters ACTIVE-DRAIN mode.

  Conditions: This may occur during aggressive session bring up or session churning and switchovers.

  Workaround: There is no workaround.

  Further Problem Description: A full reload is required to reset the system and get back to SSO HOT-STANDBY mode.

- CSCso74937

  Symptoms: In an HA setup, the active-RP may crash. Eventually, the active-SP may crash as well.

  Conditions: The symptoms are observed with a repetitive overnight ES40 linecard reset.

  Workaround: There is no workaround.

- CSCso75048

  Symptoms: The following error message is displayed:

  IPC-SP-2-ONINT: Invalid operation at interrupt level

  Conditions: Occurs while processing IPC messages for the platform multicast configuration and following the online insertion and removal (OIR) of the ES20-10GE line card.

  Workaround: Currently this error message is shown when the platform multicast subsystem tries to send too many IPC messages due to corruption in its database. Hence, a subsequent OIR or interface flap will not solve the issue. A **redundancy force-switchover** can be performed to recover from the issue.

- CSCso75456

  Symptoms: All the output packets are dropped at RSPAN destination interface.

  Conditions: Occurred while testing RSPAN with Etherchannel as destination on the Cisco 7600 router. There are no output packets on the port-channel interface which is configured as destination, although the MAC address table entry is found.

  Workaround: Perform a **shut/no-shut** of the port-channel interface after it is configured as the RSPAN destination interface.

- CSCso75863

  Symptoms: A service policy is not attached at SIP400 when attached under a virtual template in distributed link fragmentation and interleaving (dLFI) over ATM (dLFIoATM).

  Conditions: The symptom is observed with any type of QoS on a SIP400 with dLFIoATM.

Workaround: There is no workaround.

- CSCso76863

  Symptoms: With a Cisco 7600 series router, occasionally the RP may crash when a SIP or SPA is reset.

  Conditions: The symptom is observed when an RP is very busy when a SIP or SPA is reset. For example, the crash has been seen intermittently when an ESM or SPA card was reset while a large number of BGP routes are toggling.

  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.

- CSCso78716

  Symptoms: SNMP object entPhysicalVendorType returns incorrect value.

  Conditions: Occurs only on a Cisco 7603s.

  Workaround: There is no workaround.

- CSCso79720

  Symptoms: When the **show interface** command is entered, all of the Layer 2 switch port interfaces on ES-20 are shown with the same bridge MAC.

  Conditions: Only seen on ES-20.

  Workaround: As a workaround, the interface when configured to switchport, then the mac-address for the same can be correctly set by following procedure:

  a.) Execute the command **show idprom module <module> details**.

  b.) lookout for the field 'mac base' and 'mac_len' field in the output.

  c.) Assign 'mac base + port_num' as the mac-address to the port on ES20. (Ensure that 'mac base + port_num' lie within the range of 'mac base + mac_len'

  Further Problem Description: Ideally, when a port is configured as a switchport, it's desired that each port should have a unique mac-address. However, it was not like this rather all the ports were having same mac-address. which is not correct if the port is put in switchport mode. However, if all those ports which are 'not switchports' and are routed ports, they'll share the same-mac-address. It's as per the design.

- 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.

- CSCso80545

  Symptoms: If an interface changes from a down to an up state, and a better native path is available for multicast traffic, the RIB may still use the old path for multicast.

  Conditions: The symptom is observed when the **mpls traffic-eng multicast-intact** command is enabled under **router isis** *tag*. In addition, the route to the source has to be learnt over the TE tunnel.

Workaround: Use the **clear ip route** *ip prefix* command.

Further Problem Description: The MPLS TE tunnel appears to be the best path for the sources of traffic and PIM will try to use them, but an RPF check will fail because the packets are never received from TE-tunnels since they are unidirectional.

- 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.

- CSCso81370

  Symptoms: With AToM debugging enabled and a shutdown of a core interface, a crash may be experienced.

  Conditions: The symptoms are observed on a Cisco 7600 series router with AToM debugging enabled using the **debug mpls l2transport vc status ev** command, followed by a shutdown of a core interface.

  Workaround: There is no workaround.

- CSCso82707

  Symptoms: ISG radius proxy may not proxy the accounting responses back to the radius proxy client. If ISG does not receive a response for the first accounting request, it will create the session but the process will not retransmit consecutive accounting requests.

  Conditions: The symptom is observed when the AAA server goes down immediately after authentication, but before the accounting requests are sent.

  Workaround: There is no workaround.

  Further Problem Description: This has a functional impact as radius clients may think that the AAA server is down.

- CSCso85138

  Symptoms: Packets may get process switched instead of route-cache switched.

  Conditions: The symptom is observed when there is non-process switching on the interface(s) configured with Frame-Relay which results in no proper connectivity, even with the static routes, between the adjacent routers.

  Workaround: There is no workaround.

- CSCso86674

  Symptoms: Border Gateway Protocol (BGP) is unable to get route information after **shut/no shut** is performed on BGP neighbor on far-end.

  Conditions: Issue is seen when BGP is used for IPv6 routing.

  Workaround: This problem can be recovered by doing shut and no-shut again. Also, problem will not happen if you set network <prefix> at address-family on far-end router.

- CSCso87348

  Symptoms: A Catalyst 6500 or a Cisco 7600 may reload unexpectedly.

  Conditions: Occurs when NetFlow is configured on one of the following:

  * Cisco 7600 running Cisco IOS Release 12.2(33)SRC.

  * Catalyst 6500 running Cisco IOS Release 12.2SXH.

Workaround: Disable NetFlow. This is done with the following commands:

no ip flow ingress no ip flow egress no ip route-cache flow

Enter the appropriate command for each subinterface for which NetFlow is currently configured.

- CSCso87838

  Symptoms: Switch may report flapping HSRP peers when the **wr mem** command is issued.

  Conditions: The symptom is observed when HSRP is configured with aggressive timers and the **wr mem** command is issued.

  Workaround: Increase the timer values for HSRP or consider not using aggressive timers.

- 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.

- CSCso88898

  Symptoms: The line card displays memory allocation failure messages, and memory statistics indicate a continuous decline in free memory.

  Conditions: When port mode or VC mode cell relay configuration is applied on an ATM interface, it is observed that after traffic switching for a long time (approximately 48 hours, depending on scale), the above problem occurs.

  Workaround: There is no workaround.

- 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.

- CSCso89794

  Symptoms: Spurious accesses are seen when SNMP queries are performed on the router.

  Conditions: This symptom occurs if SNMP queries like "snmpwalk -v2c 7.42.19.43 public .1.3.6.1.4.1.9.3.6.13.1" are performed on the router. Spurious accesses are seen.

  Workaround: There is no workaround.

- CSCso90021

  Symptoms: If there is a port-channel configured with members from both bays and EVCs are configured on that port channel with BD, removing then adding the EVCs may then cause some of them to fail to send traffic.

Conditions: The symptom is observed when the port-channel has members from both bays and EVCs are removed and then added.

Workaround: Conduct a line card OIR.

- CSCso91230

  Symptoms: A router may display the following error:

  ```
  %LINK-2-INTVULN: In critical region with interrupt level=0, intfc=ATM0 -Process= "IGMP
  Snooping Receiving Process"
  ```

  Conditions: The symptom is observed when bridged traffic is passing to an MLPP interface.

  Workaround: Disable IGMP snooping with the **no ip igmp snooping** command.

- CSCso92175

  Symptoms: The configured value of a queue-limit gets changed and locked at 16000 bytes when random-detect is applied to the policy-map and service policy is attached to the interface.

  Conditions: The symptom is observed when a queue-limit is configured in front of the WRED in the same class of policy-map.

  Workaround: Configure the WRED in front of queue-limit in the same class of policy-map.

- 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.

- CSCso93883

  Symptoms: Upon reload of a DFC, traffic coming from the MPLS cloud might be dropped when the traffic is destined for a EoMPLS connection on a MUX-UNI

  Conditions: This is seen on 12.2(33)SRB3 and 12.2(33)SRA3. The incoming module needs to be a DFC, and the egressing port needs to be a MUX-UNI. This does not happen to regular Ethernet Over MPLS (EoMPLS) connections.

  Workaround: Perform a **shut/no shut** on the connection towards the MPLS network, then **shut/no shut** the VC.

- CSCso93959

  Symptoms: Newer SDRAM devices on the 2- and 4-port OC48 POS/RPR SPA require an additional initialization sequence as recommended by the vendor. Without this new initialization sequence, packets that go through the transit buffer in RPR/SRP mode or in subscription mode may get corrupted, or packet loss may occur.

  Conditions: Card initialization after inserting the SPA or removing an unpowered shutdown.

  Workaround: Perform an OIR on the SPA.

Customers are advised to upgrade to the newer image with this new initialization sequence. Newer software will be backward compatible with older SPA boards.

- CSCso95426

  Symptoms: In each retransmit, the AAA client explicitly shows the radius-key in the debug output, causing security concerns.

  Conditions: Occurs when RADIUS debugs are enabled, such as **debug radius all**.

  Workaround: There is no workaround. However, this is not know to impact functionality.

- CSCso97318

  Symptoms: PPPoE over VLAN over ATM functionality is broken

  Conditions: This is resulting in both PPPoE client (Cisco PPPoE test driver) and PPPoE server caching wrong PPPoE encapsulation string (with double VLAN tag). LCP CONF request from each side is not properly processed by the peer, so the session never comes up.

  Workaround: There is no workaround.

- CSCso97593

  Symptoms: Cisco ASR1000 loses QoS configuration after reload.

  Conditions: Cisco ASR1000 will lose the configuration if flat service policy is configured on Multilink Point-to-Point Protocol (MLPPP) bundles.

  Workaround: This problem is not seen if MLPPP bundles are configured with hierarchical service policy.

- CSCso97695

  Symptoms: Config replace used to fail with TFTP.

  Conditions: No special conditions.

  Workaround: TFTP copy worked fine. The workaround is to copy it and then do a config replace from the disk.

- 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.

- CSCso98964

  Symptoms: EIGRP authentication with a key string longer than 16 characters may fail. EIGRP neighbors will fail to establish.

  Conditions: Occurs in routers running a variety of Cisco IOS Release 12.2 versions.

  Workaround: Use a shorter key string.

- CSCso99860

  Symptoms: Some of the initially shipped PWR-1500-DC power supplies in Cisco 7603S chassis have incorrect SNMP OID programmed in the IDProm. The vendorOID does not match with the CANA-assigned number in CISCO-ENTITY-VENDORTYPE-OID-MIB.my

  Conditions: This is applicable for those power supplies for which the vendorOID is programmed as 193 and not as 194.

Workaround: There is no workaround.

- CSCsq02587

  Symptoms: Traffic engineering (TE) tunnel is not coming up in MPLS TE.

  Condition: Occurs when both Ethernet Over MPLS (EoMPLS) and MPLS TE are configured on the router.

  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.

- CSCsq05602

  Symptoms: Intermediate System-to-Intermediate System (IS-IS) routes still using MPLS tunnels as next hop even after tunnels are shutdown.

  Conditions: Occurs when MPLS tunnels to multiple routers are configured.

  Workaround: Use the **clear isis *** command to temporarily solve the problem.

- CSCsq05680

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

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

  Workaround: There is no workaround.

- CSCsq05997

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

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

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

  Workaround: There is no workaround.

- CSCsq06813

  Symptoms: Only one RELEASE message is seen on a DHCPv6 when the server is shut, even though multiple messages are expected.

  Conditions: The symptom occurs on Cisco 7200 series router that is running Cisco IOS Release 12.4T.

  Workaround: There is no workaround.

- 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.

- CSCsq09918

  Symptoms: Switches running REP may crash due to memory corruption (debug exception). This bug is common to ME3750, ME3400 and Cisco 7600. Multiple switches may crash.

  Conditions: This can occur when there is any traffic congestion on the REP link which causes REP EPA packets to be dropped. The problem occurs when REP link state layer retransmits the EPA packet.

  Workaround: No workaround other than solving the congestion problems on the link.

- 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.

- 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.

- CSCsq12380

  Symptoms: The SNMP engine process may experience a memory leak.

  Conditions: The symptom is observed on a Cisco 7600 series router with CEM interfaces and when the router is polled for 1.3.6.1.4.1.9.10.131.1.3.

  Workaround: Configure a SNMP view to disable polls on 1.3.6.1.4.1.9.10.131.1.3.

- CSCsq13576

  Symptoms: The router may crash when the multilink interface goes down.

  Conditions: The symptoms are observed when the multilink interface has interleave configured.

  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.

- CSCsq14031

  Symptoms: Unable to ping IP address of session target. Packets of certain sizes (between 57 and ~63 bytes, depending on the type of packet) are corrupted when using a tunnel over a PPP multilink interface. EIGRP packets were within this range and so were dropped and caused the route to the IP address being pinged not to be added.

  Conditions: Issue may be related to encryption or Network Address Translation (NAT).

  Workaround: Disable or increase the value of **ppp multilink fragmentation**.

- CSCsq14261

  Symptoms: Downstream traffic will drop when we send IPv6 traffic over PPPoE sessions.

  Conditions: Bring up a PPPoE session over L2TP tunnel for address negotiated by IPv6, then send downstream IPv6 traffic.

  Workaround: There is no workaround.

- 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.

- CSCsq15198

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

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

  Workaround: There is no workaround.

- CSCsq15994

  Symptoms: Low CPS may be observed.

  Conditions: The symptoms are seen with PPPoA and PPPoE sessions.

  Workaround: There is no workaround.

- CSCsq16008

  Symptoms: In DDP DFC, MET entries get programmed on both replication instances.

  Conditions: The symptom is observed when issuing the **shutdown** command followed by the **no shutdown** command on the interface that receives the PIM join instruction.

  Workaround: Use the **clear ipv6 pim topology** *group address* command.

- CSCsq16611

  Symptoms: IPv6 packets are process switched instead of using Cisco Express Forwarding (CEF)

  Conditions: The above symptom is observed on a Cisco 7301 and Cisco 7200 routers.

Workaround: There is no workaround.

- 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.

- CSCsq18856

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

  Conditions: This issue is seen on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsq18938

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

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

  Workaround: Disable health monitoring tests on the WS-6708

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

```
May 6 13:32:09.915 EDT: %PIM-5-NBRCHG: neighbor 10.252.3.130 DOWN on interface
Port-channel10 non DR
May 6 13:32:09.307 EDT: %CONST_DIAG-SP-6-HM_TEST_SP_INFO: TestFabricCh0Health[3]:
last_busy_percent[8%], Tx_Rate[894], Rx_Rate[2454]
May 6 13:32:09.307 EDT: %CONST_DIAG-SP-2-HM_MOD_RESET: Resetting Module 3 for software
recovery, Reason: Failed TestFabricCh0Health
May 6 13:32:09.307 EDT: %OIR-SP-3-PWRCYCLE: Card in module 3, is being power-cycled
off (Diagnostic Failure)
```

- CSCsq19146

  Symptoms: Customer seeing multiple "%SIP200_SPIRX-3-SPA_INTERRUPT: SPA 0 - seq err, SPA Int status = 0x4" errors.

  Conditions: Occurs under normal operating conditions.

  Workaround: There is no workaround.

- CSCsq19159

  Symptoms: System crash or memory corruption occurs.

  Conditions: Occurs when repeated 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.

- CSCsq21862

Symptoms: Upon the execution of the **test crash** command on the active supervisor in an HFS-capable chassis, the new active fabric channel may go out of synchronization, the traffic stops passing through the linecard, and the following error message may be seen:

%FABRIC_INTF_ASIC-5-FABRICSYNC_REQ: Fabric ASIC 0: Fabric sync requested after 3 sync errors

Conditions: The symptoms are observed on an HFS-capable chassis and are triggered by the **test crash** command on the active supervisor. It is seen with both SIP200 and SIP400.

Workaround: There is no workaround. The only way to come out of the problem state is with a line card reset using the **hw-module module** *slot* **reset** command.

- CSCsq22284

  Symptoms: A policy-map configuration may be corrupted after user entry. The "show run" output shows the corrupted policy-map configuration with (the unexpected output) "use method ssg" after "set".

  Conditions: The symptom is seen when running Cisco IOS Release 12.2(33)SRC and when configuring the policy map.

  Workaround: There is no workaround.

- CSCsq22383

  Symptoms: A Cisco 7600 router may sometimes hang while performing configuration/deconfiguration stress tests

  Conditions: Occurs on a Cisco 7600 router running Cisco IOS Release 12.2(33)SRB3.

  Workaround: There is no workaround.

- CSCsq22417

  Symptoms: A Cisco 7600 running configuration/deconfiguration tests repeatedly over time may crash.

  Conditions: Unknown conditions.

  Workaround: There is no workaround.

- CSCsq23727

  Symptoms: There may be a memory leak in the middle buffer.

  Conditions: This symptom is observed with router-generated broadcast or multicast packets alone. Use the following commands to detect the presence of this defect. 1. **show buffers leak** *inc Cc0* 2. **show buffer usage** *inc Cc0* The count will be incremented, if the problem exists.

  Workaround: There is no workaround.

- CSCsq24171

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

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

  Workaround: Reapply the configuration on the specific interface.

- CSCsq24436

  Symptoms: L2TPv3 sessions may not come up in a scaled scenario.

  Conditions: The symptom is observed when attempting to bring up more than five L2TPv3 sessions. Only half of the sessions will come up and rest remain down.

  Workaround: There is no workaround.

- CSCsq24535

  Symptoms: The tunnel stitching VC may go down resulting in traffic loss.

  Conditions: The symptom is observed when the remote peer is changed with a different MTU, causing the tunnel stitching VC to go down. When the matching MTU is reconfigured, however, the tunnel stitching session does not come back up.

  Workaround: Do a soft OIR of the Provider Edge router's interface where MTU reconfiguration is done.

- CSCsq24935

  Symptoms: A switch reloads when the **distance bgp** command is configured under ipv6 address family.

  Conditions: This symptom is observed on a Cisco 3560 that is running Cisco IOS Release 12.2(44)SE2. The same symptom is also seen on a Cisco 3750. The following commands are issued:

  router bgp <> address-family ipv6 unicast distance bgp <> <>

  The router subsequently reloads because of an Instruction access Exception.

  Workaround: There is no workaround. BGP/ipv6 is not supported on such platforms.

- CSCsq25028

  Symptoms: Malloc errors seen on enhanced FlexWANs with 256MB memory in RSP720 systems when another line card is inserted or powered up. FlexWAN I/O memory low watermark becomes very low while number of allocated IPC buffers grow in the hundreds.

  Conditions: Seen only on RSP720, not seen on SUP720 systems. Routing table has 30,000 routes or more.

  Workaround: There is no workaround.

  Further Problem Description: Inserting or powering up a line card prompts the RP to send all info to all cards and FlexWAN bays in chassis. RSP720 sends info at higher rate than FlexWAN can immediately process, so hundreds of IPC buffers are allocated until its I/O pool is exhausted and malloc error reported. May not impact operation, but risk of memory fragmentation and other failures increase.

- CSCsq26085

  Symptoms: The "total output drops" counter will no longer increment with 7600- ES20-GE3C. Instead, the increment is seen on the counter of port-channel which is in administratively down status and is not associated with the interface.

  Conditions: The symptom is observed on a 7600-ES20-GE3C that is configured with a service policy. If a port channel is created that is not associated with the interface, the drops will increment on that port-channel, instead of the expected interface.

  Workaround: Use a port-channel interface with an interface number greater than 20. For example, use "int port-channel 21".

- CSCsq27365

  Symptoms: A router can crash at l2tp_process_control_packet_cleanup.

  Conditions: Conditions are unknown at this time.

  Workaround: There is no workaround.

- CSCsq28244

  Symptoms: A new OIF VLAN may not get reprogrammed in HW after a quick link flap using the commands **shutdown** and **no shutdown**.

Conditions: The symptom is observed when the internal VLAN ID for the outgoing interface changes upon the **shutdown** and **no shutdown** command sequence.

Workaround: Use the **clear ipv6 pim topology** *group* command.

- 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.

- CSCsq28896

  Symptoms: There may be an 100 percent packet loss between hosts connected through a Cisco 7600 series router via frame-relay on different bridge groups.

  Conditions: We are still investigating the conditions for this issue. However, we estimate the following conditions: 1. Seen on Cisco IOS Release 12.2(33)SRA5-7 and Release 12.2(33)SRB3. 2. When a Cisco 7600 series router is switching traffic between bridge- domains. 3. When both ingress and egress interfaces are on the same line card and share the same LTL.

  Workaround: Use Cisco IOS Release 12.2(33)SRA4.

  Alternate Workaround: Force the traffic to be switched in software, either by disabling MLS switching, or having an ingress access-list specifying the 'log' statement. Please be cautious doing this as both workarounds may significantly impact CPU.

- CSCsq29052

  Symptoms: Packets are not forwarded out from a point-to-point (P2P) interface.

  Conditions: The symptom is observed with CEF enabled and when the P2P interface is changed from an "ip unnumbered" configuration to another interface.

  Workaround: There is no workaround.

- CSCsq29893

  Symptoms: Traffic may not flow on a port channel EVC after an OIR.

  Conditions: The symptom is observed when a port channel EVC is created with encapsulation untagged and then an OIR is performed on the linecard.

  Workaround: Reapply the configuration on the specific interface.

- 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.

- CSCsq30717

  Symptoms: A NPE-G1 resets due to a hardware watchdog timeout. This is indicated in the **show version** output with "Last reset from watchdog reset".

  Conditions: The Cisco 7200 must have an enabled PA-MC-2T3-EC with channelized T1s.

  Workaround: Disable the PA-MC-2T3-EC.

- 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.

- CSCsq31808

  Symptoms: With eiBGP multipath, incoming labeled packets may get looped in MPLS core instead of getting forwarded to CE, causing traffic issues. The following symptom may be found:

  - The error message below is frequently generated.

  ```
  Dec 17 07:44:46.734 UTC: %COMMON_FIB-3-BROKER_ENCODE: IPv4 broker failed to encode msg
  type 0 for slot(s) 0B -Traceback= 6044E470 60465864 6043BCFC 6043B570
  ```
  - The **debug cef xdr** command yields the following message:

  ```
  Mar 31 17:44:40.576 UTC: FIBrp_xdr: Table IPv4:<vrf name>, building insert event xdr
  for x.x.x.x/y. Sources: RIB Mar 31 17:44:40.576 UTC: FIBrp_xdr: Encoding path
  extensions ... Mar 31 17:44:40.576 UTC: FIBrp_xdr: - short ext, type 1, index 0 Mar 31
  17:44:40.580 UTC: FIBrp_xdr: Getting encode size for IPv4 table broker FIB_FIB xdr Mar
  31 17:44:40.580 UTC: - short path ext: len 12 Mar 31 17:44:40.580 UTC: - short path
  ext: len 24 Mar 31 17:44:40.580 UTC: - feat IPRM, len 12 Mar 31 17:44:40.580 UTC: =>
  pfx/path 113 + path_ext 24 + gsb 8 + fs 16 = 161
  ```
  - Checking the prefix, it points to drop entry.

  ```
  router#show mpls forward vrf <vrf name> x.x.x.x Local Outgoing Prefix Bytes Label
  Outgoing Next Hop Label Label or VC or Tunnel Id Switched interface 937 No Label
  x.x.x.x/y[V]  0 drop <========= it is drop
  ```
  - Checking the MOI flag of EBGP path, the No_Global flag (0x10) was incorrectly set.

  ```
  router#show ip cef vrf <vrf name> x.x.x.x int [snip] path_list contains at least one
  resolved destination(s). HW not notified path 70BFFC5C, path list 20E87B58, share 1/1,
  type recursive nexthop, for IPv4, flags resolved MPLS short path extensions: MOI flags
  = 0x16 <-------MOI flags 0x10 is incorrectly set (for ebgp path, correct flag should
  be 0x4, 0x5, 0x6 ..) correct now. [snip]
  ```
  Conditions: 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.

- CSCsq31923

  Symptoms: Crash may occur after polling MPLS-LSR-MIB mplsInterfaceConfTable.

  Conditions: MPLS-enabled tunnels exist in configuration and some are removed by doing **no int tunnel<tunnelid>**. If mibwalk of any object in mplsInterfaceConfTable is performed after that, this may result in crash.

  Workaround: Remove MPLS configuration on tunnel with the **no tunnel mode mpls traffic-eng** command before entering the **no int tunnel** command.

  Further Problem Description: It has been found this problem occurs when tunnel also contains the following config: **tunnel mpls traffic-eng path-option 1 dynamic**. Crash occurs only if image contains fix for CSCsm97259. Will see this message similar to the following before the crash:

  ```
  Jun 3 11:53:59.955 PDT: %TIB-3-GENERAL: MPLS MIB subblock ifIndex corrupted for
  ifIndex: 46 - was: 1198404176; corrected
  ```
- 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.

- CSCsq32443

  Symptoms: MCP rejecting Start-Control-Connection-Reply (SCCRP) with receive window size missing.

  Conditions: Occurs with peers that use or expect the default handling of RxWindowSize of (4) and do not include the attribute-value pair (AVP) in the SCCRQ/SCCRP messages.

  Workaround: Force peer to send AVP.

- CSCsq33677

  Symptoms: PPPoE sessions in relay mode got stuck in attempting state.

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

  Workaround: There is no workaround.

- CSCsq34195

  Symptoms: The **show ip rsvp interface** command does not provide reserved bandwidth information.

  Conditions: The symptom is observed on a Cisco 7600 series router that is running Cisco IOS Release 12.2(33)SRC in an MPLS TE environment.

  Workaround: There is no workaround.

- CSCsq36191

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

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

  Workaround: Upgrade to more memory.

- CSCsq36782

  Symptoms: In Ethernet Over MPLS (EoMPLS) environment after fast reroute (FRR) from interface on SIP600 to interface on SIP400 and re-optimization, traffic is blackholed from CPE device to core.

  Conditions: This happen only after FRR from SIP600 module to SIP400 module. FRR between SIP400 does not experience this problem.

  Workaround: There is no workaround.

- CSCsq37520

  Symptoms: A crash is seen when a child **policy-map** is added to a **policy-map** that is attached to a large number (1000s) of interfaces.

  Conditions: This symptom occurs when any configuration change results in the creation of 1000s of QoS queues at once.

  Workaround: Remove policy-map from all interfaces prior to modification.

- 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.

- CSCsq39244

  Symptoms: IPv6 traffic going to a 6PE device may be dropped after an interface flap.

  Conditions: The symptom is observed when the IPv6 prefix is known by BGP and the same prefix is assigned to the local interface. After an interface flap, the MPLS forwarded table is populated with drop and all incoming 6PE traffic going to that interface is dropped.

  Workaround: There is no workaround.

- CSCsq39254

  Symptoms: When call-home profiles are removed by the **no profile all** command, the standby system will reload if a new profile is added or a Cisco TAC profile is edited.

  Conditions: The symptom is observed when a non-default call-home profile is configured, and then removed by the **no profile all** command. The problem will occur when customer tries to add new profile or to edit a Cisco TAC profile.

  Workaround: There is no workaround.

- CSCsq40813

  Symptoms: Queue-limit locked with the given value and remains dead with "random-detect discard-class-based."

  Conditions: Happens only with random-detect discard-class-based and queue-limit configuration.

  Workaround: There is no workaround.

- CSCsq41962

  Symptoms: Unable to get ifIndexes for the GE-WAN interfaces by using SNMP.

  Conditions: The symptom occurs when ES20 and OSM exist in same chassis.

  Workaround: Use Cisco IOS Release 12.2(33)SRB3.

- CSCsq42288

  Symptoms: Scalable Ethernet over MPLS configuration and EVC configuration may not work sometimes. For Scalable EoM, the xconnect configuration has to be under SIP-400 Gig Ethernet main or sub-if.

  Conditions: Occurs under the following scenario: - some routes are learned from an IPv4 BGP session with the VC destination - the same routes are learned over an IGP session as well - initially the routes will be IGP because of better administrative distance - if the IGP session flaps, the routes will become BGP routes with VC destination being the BGP next-hop address. - when this happens this might break the VC connectivity.

  Workaround: Execute **clear ip route***VC's destination address* when the problem is seen.

- CSCsq42931

  Symptoms: Cisco 7600 series of router may reload twice when the router is booting up.

  Conditions: This is a very rare occurrence. A Cisco 7600 series might reload while it is booting up. Additionally, spurious access might be seen when linecards are booting up. These messages have no impact on functionality or stability of the router.

  Workaround: There is no workaround.

- 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.

- CSCsq44052

  Symptoms: When configuring "is-type level-1" under "router isis", the following error message may be received:

  ```
  % Ambiguous command: "is-type level-1"
  ```

  Conditions: The symptom is observed when configuring "is-type level-1" under "router isis".

  Workaround: There is no workaround.

- 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.

- CSCsq45761

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

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

  Workaround: There is no workaround.

- CSCsq47043

  Symptoms: A Cisco router functioning as the standby for an Hot Standby Routing Protocol (HSRP) group way reload when it is dissociated from that group and then re-associated with it. A sample sequence of commands that may lead to the reload is:

  [Assume that the interface in question has been previously configured with **standby** *1* ip command.]

  ```
  Router(config)#interface g0/0.30 Router(config-subif)#no standby 1 ip
  Router(config-subif)#standby 5 ip 10.10.30.105
  // wait for a while.. then:
  Router(config-subif)#no standby 5 ip 10.10.30.105 Router(config-subif)#standby 1 ip
  ```

  Conditions: The reload is seen if the triggering commands are issued when the router is part of an interdevice redundancy system and its redundancy state is HOT_STANDBY and if interdevice redundancy tracks the HSRP state of the group to which the interface belongs (in other words, **scheme standby** <*group-name*> is configured under **redundancy interdevice** configuration.

  Workaround: Remove the **scheme standby** <*group-name*><noBmdBold> command from under the **redundancy interdevice** configuration prior to configuring the **standby** <*group number*> ip command on the interface. Also save configuration, reload and then re-apply **scheme standby** <*group-name*> command.

- CSCsq47355

  Symptoms: On Cisco 7600 routers, the switch processor may crash the router when BGP is configured in rare situations.

  Conditions: This is a rare condition that can most likely happen with L3VPN and BGP recursive routes configured when a network, routing, or link event occurs (e.g., link flap in the remote ends, routing flaps, etc). This issue may also require routes to be load-balanced over multiple links.

  This issue only affects 12.2(33)SRB and 12.2(33)SRC and is fixed in 12.2(33)SRB4 and 12.2(33)SRC2 and later releases.

  Workaround: There is no workaround.

- 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.

- CSCsq48497

  Symptoms: When ingress policy map with policing action is attached to an EVC and then the **default int x/y/z** command is entered, the ingress policing does not get cleared from the hardware. When the same EVC is configured on that interface, then even without any ingress policy applied, the earlier configured policing is enabled.

  Conditions: Occurs on a ES20 interface with EVC configured. After doing the steps as above policing still works on EVC.

  Workaround: Reapply the ingress policy again on EVC, then remove the policy.

- 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.

- CSCsq50535

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

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

  Workaround: Avoid using L2PT with VPLS.

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

- 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.

- CSCsq52847

  Symptoms: Connection establishment failed with the event agent.

  Conditions: Occurs when the Event Gateway is killed and restarted on a Cisco 1812 router while running Cisco IOS Release 12.4(19.18)T2.

  Workaround: There is no workaround.

- CSCsq55273

  Symptoms: Traffic does not get shaped to parent shaper rate once the child policy is removed from the parent class.

  Conditions: Occurs on a ES20 line card. Apply a HQoS (child policy on class-default) on main interface and then remove the child policy from parent class-default. Traffic should get shaped to class-default shaper.

  Workaround: Remove and reapply the service-policy.

- CSCsq55518

Symptoms: Deletion of one sub-interface with L2TPv3 cross connect configuration may cause the others L2TPv3 sessions in other sub-interfaces to go down.

Conditions: The symptom is seen with the Cisco IOS Release 12.2(33)SRD only. It is observed when there is sub-interface with L2TPv3 cross connect configuration, such as:

```
l2tp-class vlan-class authentication password x xxxxxxxx
pseudowire-class vlan-pw encapsulation l2tpv3 protocol l2tpv3 vlan-class ip local
interface Loopback0
interface GigabitEthernet0/1.1 encapsulation dot1Q 2 xconnect 10.200.1.203 2 pw-class
vlan-pw ! interface GigabitEthernet0/1.2 encapsulation dot1Q 3 xconnect 10.200.1.203 3
pw-class vlan-pw ! The problem occurs when one sub-interface is deleted, for example:
no interface GigabitEthernet0/1.1
```

Workaround: There is no workaround.

- CSCsq55691

  Symptoms: QoS with Link Fragmentation and Interleaving (LFI) over ATM does not work.

  Conditions: Occurs after a **shut/no-shut** on the ATM interface

  Workaround: Reload the line card on both ends.

- CSCsq57462

  Symptoms: Ethernet Out of Band Channel (EOBC) hang causes line card reset. EoBC might get stuck resulting in communication loss between RP/SP and line card. This will result in line cards getting reset. This is a very rare condition and is seen only once so far.

  Conditions: Occurs during increased EoBC traffic due to convergence or link flap and is very rarely seen.

  Workaround: This impacts only one CPU. A forced switchover will recover from this condition.

- CSCsq58385

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

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

  Workaround: There is no workaround.

- 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.

- CSCsq60553

  Symptoms: An FW2 card may reload with memory version "VI4DP647228EBK-MD" installed.

  Conditions: The symptom is observed with all FW2 linecards having Memory version "VI4DP647228EBK-MD".

  Workaround: There is no workaround.

- 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.

- CSCsq62703

  Symptoms: Intermediate System-to-Intermediate System (IS-IS) tries to access invalid memory address and may cause router to stop working.

  Conditions: Occurs when a switch over happens and standby router becomes active.

  Workaround: There is no workaround.

- CSCsq63041

  Symptoms: Xconnect may not be able to be configured if "ip address" has already been configured on the interface.

  Conditions: The symptom is observed when attempting to configure IPv6 protocol demux under xconnect, when "ip address" has already been configured.

  Workaround: There is no workaround.

- CSCsq63176

  Symptoms: PA-MC-T3/E3-EC PA does not pass full traffic after a sudden burst near line rate.

  Conditions: Occurs when 256 interfaces are configured on the port adapter with multilinks operating on those serial interfaces.

  Workaround: Configure fewer than 256 serial interfaces.

- CSCsq63681

  Symptoms: Router crashes with error:

  Address Error (load or instruction fetch) exception, CPU signal 10, PC =0x4105B7D0

  Conditions: Router must be configured with fast reroute (FRR) and Netflow. More specifically the crash happens due to NetFlow learning flows (prefixes) that are taking the FRR protected path.

  Workaround: Disable NetFlow by using the following global configuration command: **no mls flow ip**.

  Additional workaround suggestions:

  1. Do not enable NetFlow on interfaces that are used by FRR. Enter **no ip flow ingress** on the interfaces. 2. Use a different FRR path that does not have interface with NetFlow enabled. 3. Do not use FRR.

  Make sure the prefixes that are learned by NetFlow are not being routed through an FRR protected path in the tunnel head end router.

- CSCsq63731

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

  Conditions: The symptoms are seen on a Cisco 2800 series and a Cisco 7200 series router when the command **vlan-dot1q** *vlan-id* is configured on the GigabitEthernet interface of a Cisco 2800 series router and **encapsulation dot1q** *vlan- id* is configured on the FastEthernet 2/1/2.1 interface.

Workaround: Change the Cisco 2800 series router's (CE) configuration to use a sub-interface for the vlan-id instead of using the **vlan- dot1q** *vlan-id* command on the main interface. With a sub-interface configured on the 2800, we can verify that the ARP packets are sent with proper VLAN ID.

- CSCsq64663

  Symptoms: Router Crashes when EtherChannel is shut down

  Conditions: Occurs on a Metro Ethernet device with over 2000 IP SLA operations configured and CFM services defined for a EtherChannel. The **no int ether-channel ...** command causes the device to crash.

  Workaround: There is no workaround.

- CSCsq67588

  Symptoms: On stateful switchover (SSO), the following message is seen on the active followed by the standby reset:

  ```
  CONST_ISSU-3-TRANSFORM_FAILED: ISSU CWAN APS Client(7003): receive transformation
  failed (ISSU_RC_NEGO_NOT_FINISHED)
  ```

  Conditions: Occurs after an SSO event.

  Workaround: There is no workaround.

- CSCsq67779

  Symptoms: Port numbering is incorrect during SNMPwalk. For example, PORT 3/1/3 is displayed as 3/0/13.

  Conditions: This is seen during SNMP walk of ES20 line cards.

  Workaround: There is no workaround.

- CSCsq67811

  Symptoms: System crashes due to I/O memory with the following error message:

  ```
  "%ETSEC-3-RECOVER_TX: Interface EOBC0/0 TX workaround invoked"
  ```

  Conditions: This condition is caused by a lockup inside the Ethernet Out of Band Channel (EOBC) MAC. This problem is rarely seen.

  Workaround: There is no workaround.

- CSCsq67817

  Symptoms: ETSEC freeze might cause router to crash due to memory depletion.

  Conditions: There is a rare hardware issue, which might lock up ETSEC driver transmit. This condition has been observed only once.

  Workaround: There is no workaround.

- 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**

- CSCsq71036

  Symptoms: On Cisco 7600 routers, a possibility exists of various error messages being seen due to memory corruption.

  Conditions: No known triggers. The error has never been reported on a Cisco 7600 router, only on Cisco 6000 routers.

  Workaround: There is no workaround.

- CSCsq73498

  Symptoms: Three MultiOS IPC processes: ciscoipc, ipc_test_admin_proc, and ipc_test_driver_proc fail with "IPC Error: send msg[3] failed ; Error - timeout" or "RPC message timed out".

  Conditions: This symptom occurs if an open IPC port is closed before the RPC response arrives.

  Workaround: Reload the router where IPC master is running.

- 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.

- CSCsq74300

  Symptoms: Loopbacks, Null0, and other non-Point-to-Point interfaces are not allowed in a **route-map set** command because of the changes introduced with caveat CSCsk63775.

  Conditions: This symptom is observed with Cisco IOS Release 12.4(18) or a later release. Upgrading to Cisco IOS Release 12.4(18) or a later release may break the existing network.

  Workaround: Use Cisco IOS Release 12.4(17) or an earlier release.

- 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.

- CSCsq75944

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

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

  Conditions: Occurs during normal use on a Catalyst 6500 or Cisco 7600. NetFlow must be enabled.

  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

- 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.

- CSCsq78100

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

  Conditions: Occurs under the following scenario:

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

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

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

- CSCsq78539

  Symptoms: When running Cisco IOS Release 12.2(33)SRC1, a buffer leak may be seen in the system buffers.

  Conditions: The symptom is observed when an ARP request needs to be sent to resolve a next hop ip address. The exact conditions required for the leak are still being investigated, however.

  Workaround: Disable the optimized CEF neighbor resolution with the following commands: **no ip cef optimize neighbor resolution no ipv6 cef optimize neighbor resolution**

- CSCsq79253

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

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

  Workaround: Reload the affected module.

- 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.

- CSCsq81116

  Symptoms: Router may reload when Optimized Edge Routing (OER) master configuration is **shut/no shut**.

  Conditions: Only occurs when OER master controller goes down and then rarely.

  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.

- CSCsq83501

  Symptoms: Router crashes while configuring more than 256 channel-groups in PA-MC-2T3-EC

  Conditions: The crash is seen after configuring more than 256 channel-groups in PA-MC-2T3-EC.

  Workaround: Do not configure more than 256 channel-groups:

- CSCsq86014

  Symptoms: When removing a subinterface on a Cisco 7600 series router, connectivity issues might occur on other subinterfaces that are part of the logical main interface.

  Conditions: The symptom is observed on an ES20 linecard and with Cisco IOS Release 12.2(33)SRB3 and Release 12.2(33)SRC1. It is seen when the configuration requires double-tagging. With a back-to-back connection, a QinQ sub-interface is created on either side and an IP address is assigned. Then, another sub-interface with the same outer VLAN is created and then removed.

  Workaround: Use the **shutdown no shutdown** command sequence to restore connectivity.

- 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.

- CSCsq87788

  Symptoms: Diagnostic TestPortLoopback is failing for OC192 SPA in Cisco IOS Release 12.2(33)SRC image.

  Conditions: Occurs with the following control plane policing (CoPP) configuration:

  In the Service-policy

Class cpp-default police cir 100000 bc 93750 be 187500 conform-action drop exceed-action drop violate-action drop

```
router#sh class-map cpp-default
Class Map match-all cpp-default (id 4) Match access-group name cpp-default
router#sh access-lists cpp-default Extended IP access list cpp-default 10 permit ip
any any (454914 matches)
```

Workaround: Remove the CoPP config, let the card boot up, and once the card is up, Apply the CoPP configuration again.

Further Problem Description: Further debugging has revealed that CoPP drops the packet. More specifically the "cpp-default" class that matches any IP address is the class which is hit and then the packet is dropped.

- CSCsq88522

  Symptoms: Convergence time is greater than expected in high availability SSO mode.

  Conditions: This issue occurs only when the **no aaa new- model** command is enabled for high available sessions such as PPPoSerial that do not need external AAA server support. This issue is observed with more than 2000 serial interfaces.

  Workaround: There is no workaround.

- 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 tap file 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.

- CSCsq93004

Symptoms: Removal of a subinterface may cause memory corruption or a crash. The symptoms are unpredictable.

Conditions: The symptoms are rare and will only be observed if a sub- interface is configured for **mpls traffic-eng auto-tunnel primary use**, and the sub-interface is later removed from the configuration.

Workaround: Do not remove sub-interfaces.

- CSCsq93507

  Symptoms: After a second switchover, forward downstream traffic rate may be limited to 100 packets per second (pps) for all the ISG IP clients put together in that VRF. Upstream traffic is not impacted and continues to be normal.

  Conditions: The symptom is observed when a Cisco 7600 series router has a SIP400 linecard on the access side, with the sub-interfaces configured with the "access" keyword and when the core is facing MPLS. After the first SSO, traffic is not impacted. After the second SSO, the downstream traffic rate may drop to 100 pps.

  Workaround: There is no workaround.

- CSCsq94036

  Symptoms: Packets are hardware-switched after applying IP precedence. The expected behavior here is that packets are software-processed when "ip precedence" is applied over "ip next-hop" because applying a policy over the other wipes the adjacencies that were already established.

  Conditions: This symptom is observed on a Cisco router that runs Cisco IOS Release 12.2SX or 12.2SR.

  Workaround: There is no workaround.

- CSCsq98626

  Symptoms: On a Cisco 7600 configured for ATM Circuit Emulation (CEM) over MPLS, there are errors reported under the CEM circuit. This is observed using the **show cem circuit** command.

  Conditions: The error is only observed when the core-facing interface has these characteristics:

  - SVI i.e L2 (Bridge-domain and Switchport) - The physical interface is from a ES20 module

  Workaround: Disable MAC address aging with the **mac-address-table aging-time 0** command.

- 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.

- CSCsr06282

  Symptoms: Causes router to reload following a SNMP get operation.

  Conditions: Only occurs when a DHCP operation is configured with option-82 parameters.

  Workaround: Do not query MIB objects relating to the DHCP operation configured with option-82

- CSCsr08750

  Symptoms: A router may crash.

Conditions: The router will crash with IO memory corruption when the **memory reserve critical [1-5]** command is executed.

Workaround: Configure the **memory reserve critical** command with a much greater size.

Further Problem Description: This issue occurs only when the ratio of free processor memory and free IO memory is high (say greater than 90).

- CSCsr08921

  Symptoms: Cisco 7600 RP crashes when pseudo-wire is down for ATM over MPLS over GRE and when AAL0 encapsulation is used. The problem happens in customer-facing SIP-400 line card.

  Conditions: Configure ATM AAL0 over MPLS over GRE, then bring the pseudo-wire down.

  Workaround: There is no workaround.

- CSCsr09173

  Symptoms: After an Not-So-Stubby Area (NSSA) ABR reload, the default LSA may fail to generate on some NSSAs.

  Conditions: The symptom is observed following a reload or other circumstances like interface flapping.

  Workaround: Reconfigure the area as NSSA by the following command sequence: **no area** *number* **nssa no- summary** followed by **area** *number* **nssa no-summary**.

- 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.

- CSCsr10893

  Symptoms: There may be high RP CPU utilization and the following message may be seen:

  ```
  %CPU_MONITOR-2-NOT_RUNNING: CPU_MONITOR messages have not been sent for 30 seconds
  ```

  Conditions: The symptom is seen with 2,000 bridge-domain EFPs and 2,000 local connect EFPS on ESM20G interfaces (xconnect is configured on each of these EVCs) and when the egress interface is shutdown using the **config t interface GigabitEthernet** *3/0/5* **shutdown** command.

  Workaround: To speed up recovery, traffic into the local connect EFPs may be stopped and restarted.

  Further Problem Description: Traffic is momentarily and wrongly punted to RP that causes RP to be busy and results in the above message. The condition is a transient one and system recovers from it in 2-3 minutes.

- CSCsr11085

  Symptoms: A single route loop whose gateway is covered by a default route remains in the RIB after a more specific route which resolves the gateway is removed. For example, the following routes may exist in the RIB:

  ```
  S* 0.0.0.0/0 is directly connected, Ethernet1/0 S 192.168.0.0/16 [1/0] via 192.168.1.2
  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.1.0/24 is directly
  connected, Ethernet0/0 L 192.168.1.1/32 is directly connected, Ethernet0/0
  192.169.1.0/24 is variably subnetted, 2 subnets, 2 masks C 192.169.1.0/24 is directly
  connected, Ethernet1/0 L 192.169.1.1/32 is directly connected, Ethernet1/0
  ```

  If interface eth 0/0 goes down, then we have the following:

```
S* 0.0.0.0/0 is directly connected, Ethernet1/0 S 192.168.0.0/16 [1/0] via 192.168.1.2
192.169.1.0/24 is variably subnetted, 2 subnets, 2 masks C 192.169.1.0/24 is directly
connected, Ethernet1/0 L 192.169.1.1/32 is directly connected, Ethernet1/0
```
and

```
Router#show ip route loop ->default:ipv4:base 192.168.0.0/16 -> base 192.168.1.2
static 00:01:07 N
```
In this case the route

```
S 192.168.0.0/16 [1/0] via 192.168.1.2
```
should be removed from the RIB.

Conditions: The default route MUST be present in order for the above behavior to be considered wrong. If a default route is NOT present then the route

```
S 192.168.0.0/16 [1/0] via 192.168.1.2
```
is a misconfiguration and must be corrected by altering the configuration. Until the configuration is corrected, the route will remain in the RIB and traffic covered by that route will be dropped.

Workaround: The one route loop can be removed from the RIB using the **clear ip route" command**:

```
clear ip route 192.168.0.0
```
Further Problem Description: In the absence of the default route removal of the one route loop can lead to oscillation, which would seriously degrade the performance of the router.

- CSCsr11099

  Symptoms: Ping fails on port-channel subinterface.

  Conditions: Routers R1, R2 connected back to back and configured as shown below. When the active link goes down or is shut, the hot standby becomes active. At this point a ping between the routers fails.

  The following conditions are necessary: - **lacp fast-switchover** is configured on the port-channel interface - Either **encapsulation dot1q** or **encapsulation isl** is configured on the port-channel subinterface - There is only one active link

  Releases affected: Cisco IOS Release 12.2SRC

  R1 R2 --- --- gi2/0/1 ------- gi2/0/1 gi2/0/2 ------- gi2/0/2

  ```
  R1 config: interface Port-channel1 no ip address lacp fast-switchover lacp max-bundle
  1
  interface Port-channel1.1 encapsulation dot1Q 38 ip address 10.1.3.1 255.255.255.0
  interface GigabitEthernet2/0/1 no ip address no mls qos trust channel-group 1 mode
  active
  interface GigabitEthernet2/0/2 no ip address no mls qos trust channel-group 1 mode
  active
  R2 config: interface Port-channel1 no ip address lacp fast-switchover lacp max-bundle
  1
  interface Port-channel1.1 encapsulation dot1Q 38 ip address 10.1.3.2 255.255.255.0
  interface GigabitEthernet2/0/1 no ip address no mls qos trust channel-group 1 mode
  active
  interface GigabitEthernet2/0/2 no ip address no mls qos trust channel-group 1 mode
  active
  ```
  Workaround: Do not configure **lacp fast-switchover**.

  Further Problem Description: This occurs because the encapsulation assigned to the new active link is set to the default "native" rather than the encapsulation configured on the port-channel subinterface. Therefore, this will cause connectivity issues even with non-routed port-channel subinterfaces.

- 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.

- CSCsr17315

  Symptoms: Autoinstall process does not run correctly with a BOOTP or DHCP server in same LAN. Because of the problem, the configuration file may not be downloaded using TFTP from the network during autoinstall.

  Conditions: The symptoms are observed with a Cisco 7200 series router that is running Cisco IOS Release 12.4(21.06)T01. It is observed with a BOOTP server and when the DHCP client and TFTP server are in same LAN. The client is configured to obtain an ip address for an interface (using the **ip address dhcp** command) and then the DHCP client configuration is copied to TFTP. The autoinstall process is started using "write erase and reload". It shows that no BOOTP information is received. The DHCP client downloads the hostname.confg file from TFTP. As a result, the configuration (using the **ip address dhcp** command) is missing on the interface.

  Workaround: There is no workaround.

- CSCsr17680

  Symptoms: AA-request, sent to a particular server, getting failed-over to all other servers in the server group, when the first server is not responding or first server is unreachable.

  Conditions: This issue is observed when sending request to particular server on a server-group.

  Workaround: There is no workaround.

- CSCsr18589

  Symptoms: A Virtual Router Redundancy Protocol (VRRP) group configured on a VLAN interface flaps from the backup to the master state after stateful switchover (SSO) when the existing master is still available on the network. The group will flap back to backup a short period later.

  Conditions: The problem only occurs when there are a large number of VLAN interfaces with a VRRP group configured on each interface and SSO is performed.

  Workaround: Each of the VRRP groups can be configured with a larger VRRP advert timer value. Values should be varied depending on the setup, but a larger than default value is usually required.

- CSCsr18942

  Symptoms: Traceback occurs when VPN routing/forwarding (VRF) is deleted and then recreated.

Conditions: Occurs when multicast RP is configured under VPN routing/forwarding (VRF) first. When the VRF is deleted, some multicast data may still be locked and not deleted, causing the traceback when a new VRF is created and multicast RP is configured there.

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.

- CSCsr20566

  Symptoms: A router may log SCHED-3-STUCKMTMR for Dampening process, after which point all dampened interfaces will be permanently dampened from a routing-protocol viewpoint.

  Conditions: This symptom is observed when multiple interfaces are configured with dampening feature.

  Workaround: There is no workaround.

- CSCsr22594

  Symptoms: Bindings assigned by the On-Demand Address Pool (ODAP) pool not synced with the standby.

  Conditions: Occurs with a Cisco 10000 as the ODAP device. Bindings of the ODAP pool are not synced with the standby.

  Workaround: There is no workaround.

- CSCsr25168

  Symptoms: Router crashes while configuring destination interface range other than available interface.

  Conditions: Configure a monitor session with destination interface range other than available interface.

  Workaround: There is no workaround.

- CSCsr27734

  Symptoms: The standby router crashes.

  Conditions: This symptom is observed when a service-policy map is removed from a VC.

  Workaround: There is no workaround.

- CSCsr28305

  Symptoms: Connectivity issues are observed when using an L2 Port-Channel on a WS-X6708-10G with two links as part of a Port-Channel.

  Conditions: Member ports of the Port-Channel are on the same module and distributed different fabric connections. Traffic stream is ingress and egress this Port-Channel. For example, default gateway configuration for multiple VLANs, so traffic is ingressing and egressing this Port-Channel when switching between VLANs.

  Workaround: For usage of a Port-Channel with two member ports use interfaces which are on the same fabric connection:

  Fabric Channel #1: Ports 2, 3, 6, 8 Fabric Channel #2: Ports 1, 4, 5, 7

- CSCsr31518

Symptoms: File copy is not working through FTP and the following error is seen:

```
%Error opening ftp://USERNAME:PASSWORD@FTP-SERVER//SOURCE_FILE DESTINATION_PATH
(Incorrect Login/Password)
```

Conditions: The symptom is observed when FTP protocol is used for copying.

Workaround: Add one more character to the password. Since this defect will drop the last character of the password, a dummy character will workaround this issue. For example, if the password is "1234", use "12345".

- CSCsr40433

  Symptoms: Traffic engineering (TE) tunnel reoptimization fails and tunnel stuck in "RSVP signaling proceeding".

  Conditions: Occurs when explicit path with loose next hops and one of the next hops is still reachable and that next hops is a dead-end.

  Workaround: Use strict next hop addresses.

- CSCsr40935

  Symptoms: Router crashes when service policy is applied while traffic is flowing.

  Conditions: Occurs on a Cisco 7200 after applying policy map on PVC with traffic.

  Workaround: Stop traffic before applying service policy map.

- CSCsr43800

  Symptoms: Router crashes on executing **vrf upgrade-cli multi-af-mode non-common-policies vrf**.

  Conditions: Occurs when **ip vrf X** is configured on an interface and execute and the **vrf upgrade-cli multi-af-mode non-common-policies vrf X** command is entered. Observed in a Cisco 7200 running Cisco IOS Release 12.2(33)SRC1.

  Workaround: There is no workaround.

- CSCsr45653

  Symptoms: CEF entry is not deleted when its neighbor is deleted.

  Conditions: The symptom occurs when netflow is configured.

  Workaround: There is no workaround.

  Further Problem Description: This issue affects memory management which in turn may impact performance.

- CSCsr45986

  Symptoms: The memory of the router may become corrupted, which can lead to a crash.

  Conditions: This symptom is observed when Flexible NetFlow is configured with a record that has a large packet section in it, and it is applied to capture traffic.

  Workaround: Configure Flexible NetFlow with a flow record that does not have a packet section in it.

  Further Problem Description: Tracebacks are observed when the following commands are issued, which leads to a Flexible NetFlow crash.

  configure terminal flow monitor mm_1 record netflow ipv4 as interface Ethernet1/0 ip flow monitor mm_1 input end

- CSCsr48422

  Symptoms: Cisco 7600 router crashes with "no ipv6 unicast-routing", during unconfiguration.

Conditions: Race condition occurs while deleting Cisco Express Forwarding (CEF) entries from a table.

Workaround: There is no workaround.

- CSCsr49316

  Symptoms: A crash happens when the **show ipv6 rpf x:x:x::x** command is given.

  Conditions: This symptom is observed only when there are more than 16 adjacencies for a single static route. The crash happens when the **show ipv6 rpf** command is given for this particular static route.

  Workaround: There is no workaround. This problem occurs as long as there are more than 16 adjacencies for single static route even if some of them are not active.

- CSCsr50821

  Symptoms: A router may crash when ARP hits through interrupt level.

  Conditions: This symptom is observed when bridging is configured, but it may also be observed when the ARP code hits by interrupt context, which is unpredictable.

  Workaround: There is no workaround.

  Further Problem Description: This defect was introduced via CSCsq05997. Cisco IOS Release 12.4 and 12.4T are not affected by this defect, but Cisco IOS Release 12.2S may be affected by this defect.

- CSCsr55278

  Symptoms: Fast switching of multicast packets may not occur on the interface of a PE router. All multicast packets are forwarded in process switching.

  Conditions: The symptom is observed after the interface is changed from a forwarding interface of one VRF to another VRF.

  Workaround: There is no workaround.

- CSCsr55865

  Symptoms: Packet marking does not work in Cisco 7200, 7200p, and 7301 ipbase images.

  Conditions: Applies to marking using "set" command. The "police" command works as expected.

  Workaround: Use a different image.

- CSCsr55990

  Symptoms: HSRP virtual MAC is dynamic instead of static on a Cisco 7600 after a reload.

  Conditions: HSRP is configured under a routed vlan-based pseudowire:

  interface Vlan X ip address 10.0.0.1 255.255.255.0 standby 1 ip 10.0.0.254 xconnect x.y.z.w encapsulation mpls

  Occurs when fast millisecond HSRP timers are used, and an HSRP interface delay is not configured.

  Workaround: Perform a **shut/no shut** on the interface "vlan X". Or, as a preventive action, configure **standby delay minimum 60** on the interfaces. Testing has shown that after a reboot the entry is installed correctly in the PFC/DFC.

- CSCsr56465

  Symptoms: Line card MAC notification test fails when redundancy mode is changed from RPR to SSO or SSO to RPR. SIP-400 Bus Connectivity Test failed when the following commands are issued:

  ```
  Conf t redundancy mode rpr
  ```

Conditions: The issue observed in the Fabric Hot Sync-enabled Sup720 and RSP720 routers Cisco IOS Release 12.2(33)SRC. In the problem state, Super Santa Ana (SSA) channels are out of sync. For example, **show platform hard ssa status** will display SSA channel status from the SSA based CWAN module console.

Workaround: There is no workaround.

- CSCsr59284

  Symptoms: Memory allocation fails. Sometimes neighbor relationship also drops.

  Conditions: Happens after entering **show mem** command. After the system booted up, while the Cisco 7600 system was receiving the BGP routes, the command is entered. Upon hitting the space key to scroll the windows for two to three times. The following errors are displayed:

  "%COMMON_FIB-3-NOMEM: Memory allocation failure for CEF: terminal fibs list in IPv4 CEF [0x08812F1C] (fatal) "

  Workaround: Enter the **show mem sum** command.

- CSCsr59719

  Symptoms: A router may crash soon after configuring **cns config initial**.

  Conditions: The symptom is observed when configuring **cns config initial** with an invalid IP address for the status URL, for example:

  ```
  router(confif)#cns config initial <any non-existent ip address> status
  http://1.1.1.1.1.1.1/junk
  ```

  When the connection to the initial server fails, the status message is posted to the status URL which will cause the router to crash if the IP address is invalid.

  Workaround: Ensure the configured ip-addresses are valid.

- CSCsr63003

  Symptoms: When SIP-400 is configured as Lawful Intercept service module, after a line card online insertion and removal (OIR), the SIP-400 may not get selected as Lawful Intercept service module.

  Conditions: Occurs when SIP-400 is configured as Lawful Intercept service module on a Cisco 7600.

  Workaround: After line card OIR, select the SIP400 again as the LI service module using the command **li-slot list <sip400 slot number>**.

- CSCsr65372

  Symptoms: Router crashes after executing **no address-family ipv4 vrf** and then **clear ip route vrf x *** commands.

  Conditions: Occurs if the commands are entered when there are still BGP prefixes in the BGP table for that VPN routing/forwarding (VRF). The router crashes at some random point of time and not necessarily immediately after executing these two commands.

  Workaround: There is no workaround.

- CSCsr67177

  Symptoms: A router may experience a corner case crash if an IPv6 OSPF router is removed from the configuration.

  Conditions: The following conditions must be met before router is removed from the configuration to experience the system crash: - OSPFv3 router does not run because the router-id is not available (it means that no IP address is available and/or router-id is not configured). - SW interface is configured, assigned under inactive OSPFv3 router, and later removed using the command **no interface ...**.

Workaround: Ensure that when the IPv6 router is configured it runs properly (if it does not start, there is a warning printed on the console advising what action to take).

- CSCsr67289

  Symptoms: Router hangs when online insertion and removal (OIR) is performed.

  Conditions: Occurs after changing the interface bandwidth followed by an OIR operation.

  Workaround: Stop traffic before making these changes.

- CSCsr72810

  Symptoms: Unidirectional traffic is dropped when the PBR is configured with "set vrf" option between global and VPN routing/forwarding (VRF).

  Conditions: Occurs under the following scenario:

  - When PBR is configured with "set vrf" option between global and VRF

  - The router is running Cisco IOS Release 12.2(33)SRC1.

  Workaround: Configure the PBR with "set vrf" option among VRFs.

- CSCsr74002

  Symptoms: In some scenarios, UDLD packets received on a dot1q tunnel port in a VLAN where a Virtual Private LAN Services (VPLS) VFI is attached may be flooded to the VPLS VLAN without being processed locally. This may lead to port being err-disabled.

  Conditions: Occurs when some port configured as dot1qtunnel port in the VPLS VLAN. It will not process the received UDLD packet on those tunnel ports and will instead send them to the VPLS. If the VLAN interface with the VFI is shutdown, UDLD is processed normally.

  Workaround: Disable UDLD or enable spanning-tree in vfi vlan.

- CSCsr74295

  Symptoms: Upon reload, static routes pointing to MLPPP interfaces do not get inserted in the RIB.

  Example: **ip route 172.16.2.2 255.255.255.255 multilink22**

  Conditions: Occurs in a router running Cisco IOS Release 12.2(33)SRC1.

  Workaround: Reconfigure the static routes being affected, or simply configure **copy run start** to initialize the routes.

- CSCsr76733

  Symptoms: When hardware EoMPLS is configured on Port-channel sub interface, traffic is not forwarded.

  Conditions: This is seen only when the member links of the port-channel are ES20 interfaces.

  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.

- CSCsr82785

  Symptoms: If APS is configured on a large number of channelized sub-interfaces associated with a single controller such that a single failure can cause all of these interfaces to failover at the same time, and RIP is configured to run over these interfaces, high sustained CPU usage will be seen following the failover and reconvergence time will be lengthy.

  Conditions: Large number of APS protected interfaces fail over at the same time. RIP is the protocol running on those interfaces. IP addresses on all interfaces are covered by the same network statement.

  Workaround: There is no workaround.

  Further Problem Description: The length of the high CPU and reconvergence period will increase as the number of impacted interfaces increases.

  The length of the high CPU and reconvergence period will also increase as the number of network statements which cover the IP addresses on the affected interfaces decreases i.e. it will be worst when a single classful network (e.g. 10.0.0.0) covers all interfaces, somewhat better when multiple classful networks are impacted.

- CSCsr86515

  Symptoms: Router crashed due to watchdog timeout in the virtual exec process:-

  ```
  %SYS-3-CPUHOG: Task is running for (128000)msecs, more than (2000)msecs
  (129/17),process = Virtual Exec. -Traceback= 40B5D8A8 40B5D984 40B5DA4C 40B5DB78
  40B5DC6C 40C0E1BC 4125D3A8 4209FAEC 420AA5A0 4054C05C 420570D8 40575510 41257298
  41257284 %SYS-2-WATCHDOG: Process aborted on watchdog timeout, process = Virtual Exec.
  -Traceback= 40B5D8C8 40B5D984 40B5DA4C 40B5DB78 40B5DC6C 40C0E1BC 4125D3A8 4209FAEC
  420AA5A0 4054C05C 420570D8 40575510 41257298 41257284
  ```

  Conditions: This was observed on a Cisco 7600 with Supervisor 720 running Cisco IOS Release 12.2(33)SRB3 after a ATM sub-interface was removed.

  Workaround: There is no workaround.

- CSCsr92184

  Symptoms: Traffic drops after VLAN change on interface configured with single VLAN BCP.

  Conditions: Unconfiguring and configuring scaled single VLAN BCP configuration with heavy traffic running can cause this to happen.

  Workaround: Perform a **shut/no shut** on all interfaces.

- CSCsr93316

  Symptoms: A Cisco 7600 router is configured with **li-slot list <slot>**. When the slot is OIR removed and re-inserted, Lawful Intercept (LI) becomes RP-based instead of being done by the line card.

  Conditions: Occurs after an online insertion and removal (OIR) operation is performed on a line card configured for LI.

  Workaround: Re-apply the li-slot list config after the line card is inserted.

- CSCsr98731

  Symptoms: If running OSPF, stale routes may be installed in the RIB. Also wrong paths (inter-area vs intra-area) are preferred.

  Conditions: Occurs on a router running Cisco IOS Release 12.2(33)SRC1.

  Workaround: There is no workaround.

- CSCsr99533

  Symptoms: Lawful Intercept (LI) may not work when accelerated LI feature is used and LI replication is being done by the supervisor card.

  Conditions: Occurs on a Cisco 7600 configured with a RSP720 supervisor card.

  Workaround: Use SIP400 as accelerated LI module.

- CSCsr99933

  Symptoms: Routers running Cisco IOS Release 12.2(33)SRB4 experiencing high CPU usage.

  Conditions: Occurs with high purge rate of 180/sec and above.

  Workaround: There is no workaround.

- CSCsu01372

  Symptoms: If "boot config disk0:<filename> nvbypass" is used, the startup configuration does not get synced 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.

- CSCsu04473

  Symptoms: Upon the first SSO switchover triggered with the **redundancy force-switchover** command, the traffic stops on the ATM N-to-1 VCC pseudowires configured with cell-packing in the direction from the MWR towards the 7600 SPA-4XOC3-ATM interface. Traffic recovers normally in the other direction.

  Conditions: Occurs on a Cisco 7600 S-series equipped with dual SUP720-3BXL. The problem is seen only when cell-packing is enabled on the N-to-1 VCC pseudowires and when APS (MR-APS) is configured on the ATM OC3 interface of the Cisco 7600 SPA-4XOC3-ATM.

  Workaround: Disable cell-packing on the ATM N-to-1 VCC pseudowires or alternatively disable APS on the SPA-4XOC3-ATM interface.

- CSCsu08935

  Symptoms: BGP as-override does not work properly on a PE to overwrite the AS in the AS4_PATH.

  Conditions: When a 4 byte CE is peered to a 2 byte capable PE using AS 23456 and the command **as-override** is configured on the neighbor, the PE router does not override the AS in the AS4_PATH with its own AS number, mapped to 4 bytes.

  Workaround: Use "allowas-in" on the CE.

- 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.

- CSCsu24087

  Symptoms: A router hangs for a couple of minutes, then crashes anytime the **clear ip bgp neighbor x.x.x in** command is issued.

Conditions: This symptom occurs when a router crashes when the **clear ip bgp neighbor x.x.x.x soft in** command is issued when the following commands are configured for that neighbor (without route-map): 1) **neighbor x.x.x.x soft-reconfiguration inbound** 2) **neighbor x.x.x.x weight** 3) **neighbor x.x.x.x filter-list in**

If any one of the commands is not configured, then the router will not crash.

Workaround: Configure route-map instead of filter-list for inbound direction. For example: "neighbor x.x.x.x filter-list 1 in" replace with "neighbor x.x.x.x route-map *name* in"

where, route-map *name* permit 10 match as-path 1

- CSCsu27109

  Symptoms: When stateful switchover (SSO) is performed on a Cisco 7600, MPLS label allocation fails.

  Conditions: Issues are seen on Cisco 7600 router. Occurs after performing the SSO. Also seeing CPU usage above 95% for 10-15 minutes.

  Workaround: There is no workaround.

- CSCsu31088

  Symptoms: Not able to execute any commands under interface after running BERT tests.

  Conditions: This issue is seen only after running SPA FPGA BERT tests and also when there is dual RP in chassis. With other BERT options, no issue is seen.

  Workaround: There is no workaround.

- CSCsu31954

  Symptoms: A router reloads.

  Conditions: Under certain crypto configurations with NetFlow also configured, the router will reload when required to fragment CEF-switched traffic on a Cisco 7200 router.

  Workaround: There is no workaround.

- CSCsu35624

  Symptoms: When a private VLAN is configured on a VTPv3 server and then deleted, the update message on a peer VTPv3 client can cause a stack overflow for VLAN manager process and crash.

  Conditions: Occurs in a Cisco 7600 running Cisco IOS Release 12.2(33)SRD.

  Workaround: There is no workaround.

- CSCsu36697

  Symptoms: The line card reloads when a line card online insertion and removal (OIR) is performed. It does not happen consistently.

  Conditions: This occurs when an empty policy is present.

  Workaround: There is no workaround.

- CSCsu39152

  Symptoms: IF-MIB registration fails as there are no free ifIndex available.

  Conditions: Occurs after an upgrade. Seen only in HA systems.

  Workaround: There is no workaround.

- CSCsu40667

  Symptoms: A Cisco 7600 series router may fail to install some NetFlow entries even if NetFlow table utilization is low.

Conditions: Occurs while flows are ingressing on ES20 module.

Workaround: There is no workaround.

Further Problem Description: The **show mls netflow table-contention detail** command will show a heavy ICAM table utilization, while TCAM utilization is small.

```
Router#sh mls net table-contention det
Earl in Module 1
Detailed Netflow CAM (TCAM and ICAM) Utilization
================================================
TCAM Utilization : 0%
ICAM Utilization : 98%
Netflow TCAM count : 152
Netflow ICAM count : 126
Netflow Creation Failures : 388663
Netflow CAM aliases : 0
```

- CSCsu42315

  Symptoms: When the L3VPN prefix uses a tunnel with fast reroute (FRR) protection, there is traffic loss during reoptimization.

  Conditions: Not all prefix in the VRF will observe this issue. This is seen only when there are more than 250,000 prefixes.

  Workaround: There is no workaround.

  Further Problem Description: Traffic loss during re-optimization can be due to faster tunnel cleanup also. It is advisable to configure **mpls traffic-eng reoptimize timers delay cleanup** <*seconds*> to fine tune the cleanup according to the topology.

- CSCsu44992

  Symptoms: VPDN redirect functionality does not work.

  Conditions: Basic functionality is broken. No special condition is required.

  Workaround: There is no workaround.

- CSCsu46822

  Symptoms: When account logon is done for a DHCP user, QoS policies defined in the user profile are not applied to the ISG session.

  Conditions: A DHCP session is created. User performs account logon via SESM (not CoA). User profile has QoS polices defined. Session is authenticated but policies are not applied to the session.

  Workaround: Perform account logon using CoA.

- CSCsu47037

  Symptoms: Router crashes when an attempt is made to forward a packet out of an Auto-Template interface.

  Conditions: This occurs when the interface's MTU is set to 0: Use the **show interface Auto-Template X** command to show the MTU.

  Workaround: Configure a protocol MTU directly on the Auto-Template interface.

- CSCsu49790

  Symptoms: PVC range disappears after a second PVC range is configured.

  Conditions: Occurs under the following scenario:

  1) Configure a PVC range on a point-to-point interface.

  2) Configure a second PVC range that approaches the maximum number of VCs possible.

Workaround: There is no workaround.

- CSCsu50118

  Symptoms: More convergence time seen even with the **carrier-delay msec 0** command configured.

  Conditions: Occurs when **carrier-delay msec 0** is configured on a gigabit interface.

  Workaround: If excessive convergence time is observed even with the **carrier-delay msec 0** command configured, enter the command again on the interface.

- CSCsu51095

  Symptoms: If connected routes are optimized using PfR, there will be a routing loop.

  Conditions: This symptom can occur if, for some reason, PfR is learning connected routes or if the user has configured them.

  Workaround: Create an oer-map with a prefix-list that contains the prefixes with the IP addresses of the connected routes (the next hops). Set the set observe mode in the oer-map.

- CSCsu51245

  Symptoms: Port-channel QinQ subinterface on ESM20 and SIP600 line cards do not pass traffic after router reload and line card reset.

  Conditions: This condition is seen after router reload or member link line card reset. This is not seen when configuration is newly applied.

  Workaround: To recover from the condition, perform a **shut/no shut** on the port channel main interface.

- CSCsu55883

  Symptoms: With MLPPP configured on OSM, the following symptoms may be observed:

  1. Line card might crash.

  2. Links might flap.

  3. Following error message from line card might be seen:

  ```
  "SLOT 9: Sep 14 13:48:48.479 CDT: %COMMON_FIB-3-FIBIDBINCONS2: An internal software
  error occurred. Multilink1 linked to wrong idb R11_Mu1"
  ```

  Conditions: Occurs on routers running various Cisco IOS Release 12.2SR releases. Performing a **shut/no shut** on the OSM (especially on the card containing MLPPP) interfaces might trigger this issue.

  Workaround: There is no workaround.

- CSCsu57331

  Symptoms: In a Virtual Private LAN Services (VPLS) scenario with ESM20 as core facing interface, imposition traffic might fail.

  Conditions: Occurs only when ports from Bay 1 are used as core facing interface.

  Workaround: Reset the line card.

- CSCsu57958

  Symptoms: In a scenario where a Catalyst 6500 or Cisco 7600 performs DHCP snooping + DAI functionality and a second device acts as DHCP relay, it was observed that DHCP snooping database was not populated. DHCP snooping is configured in this case on the ingress VLAN (traffic from the DHCP clients) and the DHCP server can be reached on a different egress VLAN (DHCP requests are routed).

DHCP Replies from the server (DHCPOFFER and DHCPACK) are not snooped by the Catalyst 6500 or Cisco 7600 and so bindings are not established. Consequence is that clients will get their own IP Address but ARP Inspection will fail because bindings were not learned on the device.

Conditions: Occurs with DHCP Snooping + DAI configured on a Catalyst 6500 or Cisco 7600 in a routed scenario (Ingress VLAN and Egress VLAN are different) and DHCP Relay performed by a different device.

Workaround: Configure DHCP Snooping on both client and server side VLANs. Problem is applicable to both Cisco IOS Release 12.2(18)SXF and Cisco IOS Release 12.2(33)SRB.

- CSCsu65189

  Symptoms: If router is configured as follows:

  ```
  router ospf 1 ... passive-interface Loopback0
  ```
  And later is enabled LDP/IGP synchronization using command

  ```
  Router(config)#router ospf 1
  Router(config-router)# mpls ldp sync
  Router(config-router)#^Z
  ```
  MPLS LDP/IGP synchronization will be allowed on interface loopback too.

  ```
  Router#sh ip ospf mpls ldp in Loopback0 Process ID 1, Area 0 LDP is not configured
  through LDP autoconfig LDP-IGP Synchronization : Required < ---- NOK Holddown timer is
  not configured Interface is up
  ```
  If the **clear ip ospf proc** command is entered, LDP will keep the interface down. Down interface is not included in the router LSA, therefore IP address configured on loopback is not propagated. If some application like BGP or LDP use the loopback IP address for the communication, application will go down too.

  Conditions: Occurs when interface configured as passive. Note: all interface types configured as passive are affected, not only loopbacks.

  Workaround: Do not configure passive loopback under OSPF. Problem only occurs during reconfiguration.

  The problem will not occur if LDP/IGP sync is already in place and: - router is reloaded with image with fix for CSCsk48227 - passive-interface command is removed/added

- CSCsu65225

  Symptoms: TFTP from supervisor to ACE modules fail.

  Conditions: Results in the inability to copy/upgrade images to standby ACE. This is due to moving all 127.x.x.x addresses in an internal VPN routing/forwarding (VRF), which causes TFTP to fail.

  Workaround: ACE modules could fail-over to make standby as active and then ftp from the server directly.

- CSCsu77549

  Symptoms: Protocol Independent Multicast (PIM) VPN routing/forwarding (VRF) neighbors not formed.

  Conditions: Occurs after line card reload.

  Workaround: Delete and add back the MVPN configuration.

- CSCsu83563

  Symptoms: Multicast rate-limiters stop working after a HA switchover.

  Conditions: To see this issue you have to have a HA setup with multicast rate-limiters set. In order to see this issue the rate-limiters must have been set before the standby is booted. If the rate-limiters are set after standby is up in HOT state, the issue is not seen after switchover.

Workaround: Remove and reconfigure the rate-limiters.

- CSCsu94030

  Symptoms: Internal VRF gets disabled at when the router boots up.

  Conditions: Occurs after any failover or router start-up scenario

  Workaround: Use the **no platform ivrf disable** to avoid the issue.

- CSCsu94720

  Symptoms: Router crashes when the **shutdown** command is used on an interface.

  Conditions: Occurs when there are DHCPv6 bindings.

  Workaround: There is no workaround.

- CSCsu96649

  Symptoms: On Cisco 7600 with RSP720-3C-10GE processor, if the SIP-400 is configured as Lawful Intercept (LI) service module after a line card online insertion and removal (OIR), the SIP-400 may not get selected as Lawful Intercept service module.

  Conditions: Occurs when the SIP-400 is configured as Lawful Intercept service module on the Cisco 7600.

  Workaround: After line card OIR, select the SIP-400 again as the LI service module using the command **li-slot list** <*sip400 slot number*>.